Release Notes for Cisco IOS Release 15.2M&T

First Published: July 22, 2011
Last Updated: October 24, 2016
Release: Cisco IOS Release 15.2.4M11

These release notes support Cisco IOS Release 15.2M&T up to and including Cisco IOS Release 15.2.4M11. The release notes are updated with each 15.2M&T release to describe new features and related documents.

Cisco IOS Release 15.2M&T provides the latest innovations for the world’s most demanding networks and is designed to provide a unified network architecture that is stable, reliable, and secure. New features are fully integrated with extensive capabilities already available in Cisco IOS software to provide solutions for enterprise, service provider, and smart-grid.

Contents

This document contains the following sections:

- Cross-Platform System Requirements, page 2
- MIBs, page 3
- Field Notices and Software-Related Tools and Information, page 4
- Troubleshooting, page 4
- Feature Support, page 5
- Memory Recommendations, page 6
- Platform-Specific Information, page 7
- New and Changed Information, page 17
- Important Notes, page 56
- Open and Resolved Bugs, page 77
- Related Documentation, page 565
- Notices, page 565
- Obtaining Documentation and Submitting a Service Request, page 567
Cross-Platform System Requirements

This section describes the system requirements for Cisco IOS Release 15.2M&T and includes the following sections:

- Supported Hardware Platforms, page 2
- Determining Your Software Version, page 2
- Upgrading to a New Release, page 2

Supported Hardware Platforms

Cisco IOS Release 15.2M&T supports platforms within the following Cisco series:

- Cisco 800 series routers
- Cisco 1800 series routers (1861E)
- Cisco 1900 series integrated services routers
- Cisco 2900 series integrated services routers
- Cisco 3900 series integrated services routers
- Cisco 7200 Series Routers
- Cisco 7300 Series Routers
- Cisco Connected Grid Router (CGR) 2000 series
- Cisco High Density Analog Voice Gateways

For more information about the platforms supported in Cisco IOS Release 15.2M&T, see the “Platform-Specific Information” section on page 7.

Determining Your Software Version

To determine the version of Cisco IOS software that is currently running on your Cisco network device, log in to the device and enter the `show version` user EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software IOS (tm)
15.2 Software (c880data-universalk9-mz), Version 15.2(1)T, RELEASE SOFTWARE
```

Upgrading to a New Release

For information about selecting a new Cisco IOS software release, see How to Choose a Cisco IOS Software Release at the following URL:


For information about updating or upgrading Cisco IOS Software, see How to Update/Upgrade Cisco IOS Software at the following URL:

Platform-specific documents may also provide information about upgrading to a new software release:

- Cisco 800 series routers:
- Cisco 1800 series routers:
- Cisco 1900 series routers:
- Cisco 2900 and 3900 series routers:
- Cisco Connected Grid Routers 2010:

For instructions on ordering a Cisco IOS upgrade, see the document at the following location:


To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/cfn

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

**MIBs**

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

Field Notices and Software-Related Tools and Information

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at http://www.cisco.com/cisco/software/navigator.html?a=a&i.rpm.

Troubleshooting

The following documents and websites provide assistance with troubleshooting your Cisco hardware and software:

- Troubleshoot and Alerts Product Selection Page
  http://www.cisco.com/cisco/web/psa/troubleshoot.html?mode=prod&level0=268437899
- Hardware Troubleshooting Index Page
- Cisco 800 Series Routers Troubleshooting Guides
- Troubleshooting Cisco 3900 Series, 2900 Series, and 1900 Series ISRs
- Cisco Unified Communications 500 Series Install and Upgrade Tech Notes
- Cisco IOS System Message Guide
- Cisco Support Community
  https://supportforums.cisco.com/index.jspa
Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains specific Cisco IOS features.

Caution
Cisco IOS images with strong encryption (including, but not limited to 168-bit [3DES] data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Feature-to-image mapping is available through Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). You can compare Cisco IOS software releases side-by-side to display both the features unique to each software release and the features that the releases have in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

www.cisco.com/go/cfn

For help with Cisco Feature Navigator, see the help information at the following URL:


Determining the Software Images (Feature Sets) That Support a Specific Feature

To determine which software images (feature sets) in a Cisco IOS release support a specific feature, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1
From the Cisco Feature Navigator home page, click Research Features.

Step 2
Select your software type or leave the field as “All”.

Step 3
To find a feature, you can search by either Feature or Technology (select the appropriate button). If you select Search by Feature, you can further filter your search by using the Filter By text box.

Step 4
Choose a feature from the Available Features text box, and click the Add button to add the feature to the Selected Features text box.

Note
To learn more about a feature in the list, click the View Desc button in the Available Features text box.

Repeat this step to add features. A maximum of 20 features can be chosen for a single search.

Step 5
Click Continue when you are finished choosing features.
Release Notes for Cisco IOS Release 15.2M&T

Memory Recommendations

Step 6  In the Release/Platform Tree area, select either your release (from the Train-Release list) or your platform (from the Platform list).

Step 7  The “Search Result” table will list all the software images (feature sets) that support the features that you chose.

Note  You can download your results into an Excel spreadsheet by clicking on the Download Excel button.

Determining the Features Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set), go to the Cisco Feature Navigator home page and perform the following steps.

Step 1  From the Cisco Feature Navigator home page, click Research Software.

Step 2  Select your software type from the drop-down list and chose the Release button in the “Search By” area.

Step 3  From the Major Release drop-down list, chose the appropriate major release.

Step 4  From the Release drop-down list, choose the appropriate maintenance release.

Step 5  From the Platform drop-down list, choose the appropriate hardware platform.

Step 6  From the Feature Set drop-down list, choose the appropriate feature set. The Image Details area will provide details on the specific image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.

Note  To learn more about a feature in the list, click the View Desc button in the Available Features text box.

Memory Recommendations

To determine memory recommendations for software images (feature sets) in your Cisco IOS release, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1  From the Cisco Feature Navigator home page, click Research Software.

Step 2  Select your software type from the drop-down list and choose the Release button in the “Search By” area.

Step 3  From the Major Release drop-down list, choose the appropriate major release.

Step 4  From the Release drop-down list, choose the appropriate maintenance release.

Step 5  From the Platform drop-down list, choose the appropriate hardware platform.

Step 6  From the Feature Set drop-down list, choose the appropriate feature set.
The Image Details area will provide details on the specific image including the DRAM and flash memory recommendations for each image. The Available Features area will list all the features that are supported by the feature set (software image) that you chose.

**Platform-Specific Information**

Cisco IOS Release 15.2M&T supports the following Cisco series:

- Cisco 800 Series Routers, page 8
- Cisco 1800 Series Integrated Services Routers, page 9
- Cisco 1900 Series Integrated Services Routers, page 10
- Cisco 2900 Series Integrated Services Routers, page 11
- Cisco 3900 Series Integrated Services Routers, page 12
- Cisco 7200 Series Routers, page 13
- Cisco 7300 Series Routers, page 14
- Cisco Connected Grid Router 2000 Series, page 15
- Cisco High Density Analog Voice Gateways, page 16
Cisco 800 Series Routers

Cisco IOS Release 15.2M&T supports the following Cisco 800 series routers:

- Cisco 812G, Cisco 812G-CIFI
- Cisco 819G
- Cisco 819H, Cisco 819HG, Cisco 819HGW, Cisco 819HW
- Cisco 861
- Cisco 866VAE
- Cisco 867VAE
- Cisco 886VA, Cisco 886VAG, Cisco 886VA-W, Cisco 886-CUBE
- Cisco 887, Cisco 887VA, Cisco 887VAG, Cisco 887VAGW, Cisco 887VAMG, Cisco 887VA-M, Cisco 887VA-W, Cisco 887VA-WD, Cisco 887VAM-W, Cisco 887-CUBE
- Cisco 888, Cisco 888E, Cisco 888EA, Cisco 888EG, Cisco 888SRST, Cisco 888-CUBE (Cisco 888EA is supported in Cisco IOS Release 15.2(2)T and later releases)
- Cisco 891
- Cisco 892, Cisco 892 FSP, Cisco 892F-CUBE
- Cisco 896VA
- Cisco 897VA, Cisco 897VA-M, Cisco 897VA-W, Cisco 897VAM-W
- Cisco 898EA

For detailed information about the Cisco 800 series of routers, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Cisco 1800 Series Integrated Services Routers

Cisco IOS Release 15.2M&T supports the following Cisco 1800 series integrated services routers:

- Cisco 1861E

For detailed information about the Cisco 1800 series integrated service routers, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Cisco 1900 Series Integrated Services Routers

Cisco IOS Release 15.2M&T supports the following Cisco 1900 series integrated services routers:

- Cisco 1905
- Cisco 1906C
- Cisco 1921
- Cisco 1941
- Cisco 1941W

For detailed information about the Cisco 1900 series integrated service routers, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Cisco 2900 Series Integrated Services Routers

Cisco IOS Release 15.2M&T supports the following Cisco 2900 series integrated services routers:

- Cisco 2901
- Cisco 2911
- Cisco 2921
- Cisco 2951

For detailed information about the Cisco 2900 series of routers, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Cisco 3900 Series Integrated Services Routers

Cisco IOS Release 15.2M&T supports the following Cisco 3900 series integrated services routers:

- Cisco 3925
- Cisco 3925E
- Cisco 3945
- Cisco 3945E

For detailed information about the Cisco 3900 series of routers, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Cisco 7200 Series Routers

Cisco IOS Release 15.2M&T supports the following Cisco 7200 series routers:

- Cisco 7200
- Cisco 7200-NPE-G2
- Cisco 7201

For detailed information about the Cisco 7200 series of routers, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Cisco 7300 Series Routers

Cisco IOS Release 15.2M&T supports the Cisco 7301 router.

For detailed information about the Cisco 7300 series of routers, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Cisco Connected Grid Router 2000 Series

Cisco IOS Release 15.2M&T supports the Cisco Connected Grid Router 2010 (CGR 2010).

For detailed information about Cisco Connected Grid Routers, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Cisco High Density Analog Voice Gateways

Cisco IOS Release 15.2M&T supports the Cisco VG350 High Density Voice over IP Analog Gateway. For detailed information about Cisco analog voice gateways, see the documents at the following location:


For additional information about supported hardware for this platform and release, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Memory recommendations and feature support information for Cisco IOS Release 15.2M&T are also available through Cisco Feature Navigator.
Contents

These release notes describe the following topics:

- New and Changed Information, page 17
- Important Notes, page 26

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.2M&T and contains the following subsections:

- New Hardware Features Supported in Cisco IOS Release 15.2(4)M7, page 18
- New Software Features Supported in Cisco IOS Release 15.2(4)M7, page 18
- New Hardware Features Supported in Cisco IOS Release 15.2(4)M6, page 18
- New Software Features Supported in Cisco IOS Release 15.2(4)M6, page 18
- New Hardware Features Supported in Cisco IOS Release 15.2(4)M5, page 18
- New Software Features Supported in Cisco IOS Release 15.2(4)M5, page 18
- New Hardware Features Supported in Cisco IOS Release 15.2(4)M4, page 18
- New Software Features Supported in Cisco IOS Release 15.2(4)M4, page 18
- New Hardware Features Supported in Cisco IOS Release 15.2(4)M3, page 18
- New Software Features Supported in Cisco IOS Release 15.2(4)M3, page 18
- New Hardware Features Supported in Cisco IOS Release 15.2(4)M2, page 19
- New Software Features Supported in Cisco IOS Release 15.2(4)M2, page 19
- New Hardware Features Supported in Cisco IOS Release 15.2(4)M, page 20
- New Software Features Supported in Cisco IOS Release 15.2(4)M, page 21
Note
A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://www.cisco.com/go/cfn.

New Hardware Features Supported in Cisco IOS Release 15.2(4)M7
There are no new hardware features supported in Cisco IOS Release 15.2(4)M7.

New Software Features Supported in Cisco IOS Release 15.2(4)M7
There are no new software features supported in Cisco IOS Release 15.2(4)M7.

New Hardware Features Supported in Cisco IOS Release 15.2(4)M6
There are no new hardware features supported in Cisco IOS Release 15.2(4)M6.

New Software Features Supported in Cisco IOS Release 15.2(4)M6
There are no new software features supported in Cisco IOS Release 15.2(4)M6.

New Hardware Features Supported in Cisco IOS Release 15.2(4)M5
There are no new hardware features supported in Cisco IOS Release 15.2(4)M5.

New Software Features Supported in Cisco IOS Release 15.2(4)M5
There are no new software features supported in Cisco IOS Release 15.2(4)M5.

New Hardware Features Supported in Cisco IOS Release 15.2(4)M4
There are no new hardware features supported in Cisco IOS Release 15.2(4)M4.

New Software Features Supported in Cisco IOS Release 15.2(4)M4
There are no new software features supported in Cisco IOS Release 15.2(4)M4.

New Hardware Features Supported in Cisco IOS Release 15.2(4)M3
This section describes new and changed features in Cisco IOS Release 15.2(4)M3. Some features may be new to Cisco IOS Release 15.2(4)M3 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in
Cisco IOS Release 15.2(4)M3. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

**SM-X-1T3/E3 (Secure Boot)**

For detailed information about this feature, see the following document:

**New Hardware Features Supported in Cisco IOS Release 15.2(4)M2**

This section describes new and changed features in Cisco IOS Release 15.2(4)M2. Some features may be new to Cisco IOS Release 15.2(4)M2 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(4)M2. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

**High Density FXS Module Support on ISR G2**

For detailed information about this feature, see the following document:

**New Software Features Supported in Cisco IOS Release 15.2(4)M2**

This section describes new and changed features in Cisco IOS Release 15.2(4)M2. Some features may be new to Cisco IOS Release 15.2(4)M2 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(4)M2. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

**Cisco VG350 No Payload Encryption (NPE) Image**

For detailed information about this feature, see the following document:

**Flexible NetFlow: Integration with MQC**

For detailed information about this feature, see the following document:
New and Changed Information

Flexible NetFlow: IPFIX Export Format

For detailed information about this feature, see the following document:

MACE Phase-2 Enhancements

For detailed information about this feature, see the following document:

NBAR2 Custom Protocol

For detailed information about this feature, see the following document:

Protocol Pack Licensing

For detailed information about this feature, see the following document:

New Hardware Features Supported in Cisco IOS Release 15.2(4)M

This section describes new and changed features in Cisco IOS Release 15.2(4)M. Some features may be new to Cisco IOS Release 15.2(4)M but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(4)M. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

High Density Analog Gateway

For detailed information about this feature, see the following document:

Multimode 4G LTE for Cisco 819 ISRs and eHWICs

For detailed information about this feature, see the following documents:
Cisco 819 Hardware Installation Guide:
Cisco 819 Software Configuration Guide:
Cisco 819 4G LTE Integrated Services Routers Release Notes:
4G LTE EHWIC Hardware Installation Guide:
4G LTE EHWIC Software Configuration Guide:
4G LTE EHWIC Release Notes:

WLAN Support on 819 Series ISR G2 Routers

For detailed information about this feature, see the following documents:

New Software Features Supported in Cisco IOS Release 15.2(4)M

This section describes new and changed features in Cisco IOS Release 15.2(4)M. Some features may be new to Cisco IOS Release 15.2(4)M but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(4)M. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

BFD Support for EIGRP IPv6

For detailed information about this feature, see the following document:

BGP: Graceful Shutdown (GSHUT)

For detailed information about this feature, see the following document:
**New and Changed Information**

**Cisco IP Multiplexing**
For detailed information about this feature, see the following document:

**CME, SRST Version 9.1**
For detailed information about this feature, see the following documents:

**EIGRP Route Tag Enhancements**
For detailed information about this feature, see the following document:

**GET VPN Support with Suite B**
The GET VPN Support with Suite B feature adds support of the Suite B set of ciphers to Cisco Group Encrypted Transport (GET) VPN.

Suite B is a set of cryptographic algorithms that includes AES as well as algorithms for hashing, digital signatures, and key exchange. Suite B for IPsec VPNs is a standard and has been defined in RFC 4869. Suite B provides a comprehensive security enhancement for Cisco IPsec VPNs, and it enables additional security for large-scale deployments. Suite B is the recommended solution for organizations requiring advanced encryption security for the wide-area network (WAN) between remote sites.

The GET VPN Support with Suite B feature introduces or modifies the following commands: client rekey hash, group size, identifier, rekey sig-hash algorithm, and show crypto gdoi.

**IKEv2 Load Balancer Support**
For detailed information about this feature, see the following document:

**IPSLA Multicast Support**
For detailed information about this feature, see the following document:

**IS-IS IPv6 Administrative Tag**
For detailed information about this feature, see the following document:
IS-IS IPv6 Advertise Passive Only

For detailed information about this feature, see the following document:

Metadata NBAR Integration

For detailed information about this feature, see the following document:

Multiple Destination Pattern Support on Voice Dial Peer

For detailed information about this feature, see the following document:

Multiple PPPoE Clients Support on PVC with Configurable MAC Address

For detailed information about this feature, see the following document:

NTPv4 MIB

For detailed information about this feature, see the following document:

OSPFv3 MIB

For detailed information about this feature, see the following document:

OSPFv3 VRF-Lite/PE-CE

For detailed information about this feature, see the following document:

Proxy Mobile IPv6 Support for MAG Functionality

For detailed information about this feature, see the following document:
Raw Socket Transport

For detailed information about this feature, see the following document:

Routed Pseudowire and Routed VPLS

For detailed information about this feature, see the following document:

RSVP over UDP

For detailed information about this feature, see the following document:

ScanSafe Web Security

For detailed information about this feature, see the following document:

Note
The ISR Web Security with Cisco ScanSafe feature in this IOS release is under controlled availability. If you intend to use this feature please contact your Cisco representative. He or she will provide you the necessary guidance in implementing this feature into your network. For additional information please contact us at ss-isr-connector-sales@cisco.com.


The IPSec algorithms required by Suite B are now supported by the hardware crypto engine on the Cisco Integrated Services Routers Generation 2: 800 Series, 1900 Series, 2901, 2911, 2921, 2935R, 3925E, and 3945E, each of which has embedded hardware-accelerated VPN encryption.

Suite B requirements comprise four user-interface suites of cryptographic algorithms for use with IKE and IPSec, which are described in RFC 6379 and RFC 6380. Each suite consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm.

Suite B provides a comprehensive security enhancement for Cisco IPSec VPNs, and it allows additional security for large-scale deployments. Suite B is the recommended solution for organizations requiring advanced encryption security for the wide-area network (WAN) between remote sites.

For detailed information about Cisco IOS IPSec features in 15.2(4)M that support Suite B, see the following documents:
TCP—Configurable Keepalive Timer

For detailed information about this feature, see the following document:


UCS-E Series Server

The Cisco UCS E-Series Server Modules (E-Series Servers) are the next generation of Cisco UCS Express servers. E-Series Servers are a family of size, weight, and power efficient blade servers that are housed within the Generation 2 Cisco Integrated Services Routers (ISR G2). E-Series Servers provide the following:

- A general purpose compute platform for branch-office applications deployed either on the Microsoft Windows or Linux operating systems, or deployed as virtual machines on hypervisors, such as VMware vSphere or Microsoft Hyper-V.
- A hosting platform for virtualized Cisco branch-office services, such as Cisco Virtual Wide Area Application Services (vWAAS), Cisco Unified Communications Manager (Unified CM), and Cisco Enterprise Content Delivery System (ECDS).

VPN ISM IPv6 Support

The VPN ISM IPv6 Support feature enables IPv6 capability on Reventon so that IPsec IPv6 traffic is offloaded along with IPsec IPv4 traffic to the Integrated Services Module (ISM). Reventon is an ISM that delivers a peak rate of 600 Mbps IPsec encryption and decryption on Integrated Services Routers Generation 2 (ISR G2) devices.

The IPsec packet pool size is currently 256 bytes. However, with a jumbo packet of 9000 bytes and low Maximum Transmission Unit (MTU) on the router, Reventon runs out of packet buffer in IPsec packet pool and crashes.

Note: The VPN ISM IPv6 Support feature does not support high availability (HA) and IPv6 dynamic crypto maps.
**VRRPv3 Protocol Support**

For detailed information about this feature, see the following document:


**Zero Touch Recovery**

Compact flash cards can help you configure new or replacement routers, and to recover the configuration of a failed router. For example, if the Connected Grid Swap Drive feature is enabled, you can transfer the same system configuration information from one router to another by using a compact flash memory card (or compact flash card) while the routers are operating. This is done by inserting an optional compact flash card in slot CF1 and copying all contents of CF0. After the copy operation is completed, you can remove and insert this compact flash card unit in slot CF0 of either a new router or a replacement router for a failed unit. When the new or replacement router is rebooted, it uses the configuration from the compact flash card as the running and startup configuration. This functionality enables you to quickly configure new or replacement routers with a standard configuration with little or no manual configuration required.

For detailed information about this feature, see the following document:


**Important Notes**

The following information applies to all releases of Cisco IOS Release 15.2(4)M.

- Important Notes for Cisco IOS Release 15.2(4)M, page 26
- Cisco IOS Behavior Changes, page 27

**Important Notes for Cisco IOS Release 15.2(4)M**

This section describes important issues that you should be aware of for Cisco IOS Release 15.2(4)M and later releases.

**Images Deferred Because of Caveat CSCub34396**

In Cisco IOS Release 15.2(4)M, images for all platforms have been deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCub34396; Headline: traffic flow in dmvpn is flowing unencrypted.

The software solution for these deferred images is Cisco IOS Release 15.2(4)M1.

Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.
ScanSafe Web Security

The ISR Web Security with Cisco ScanSafe feature is under controlled availability in Cisco IOS Release 15.2(4)M and later releases. If you intend to use this feature please contact your Cisco representative. He or she will provide you the necessary guidance in implementing this feature into your network. For additional information please contact us at ss-isr-connector-sales@cisco.com.

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

Behavior changes are provided for the following releases:

- Cisco IOS Release 15.2(4)M4, page 27
- Cisco IOS Release 15.2(4)M3, page 28
- Cisco IOS Release 15.2(4)M2, page 29

Cisco IOS Release 15.2(4)M4

The following behavior changes are introduced in Cisco IOS Release 15.2(4)M4:

- The `radius-server attribute 66 include-in-access-req` and `radius-server attribute 67 include-in-access-req` commands are added to identify the PPTP tunnel-specific information.

  Old Behavior: The RADIUS server does not have Point-to-Point Tunneling Protocol (PPTP) tunnel-specific information because the tunnel-client endpoint and tunnel-server endpoint attributes are missing in the access-request packets sent to the RADIUS server.

  New Behavior: The following commands are introduced to identify the hostname or address of the network access server (NAS) at the initiator and server end of the Point-to-Point Tunneling Protocol (PPTP) tunnel by sending the Tunnel-Client-Endpoint attribute and the Tunnel-Server-Endpoint attribute in access-request packets to the RADIUS server.

  - `radius-server attribute 66 include-in-access-req`
  - `radius-server attribute 67 include-in-access-req`

  Additional Information:
  

- Installing simultaneous QoS policies on both ATM subinterface and ATM PVC, or on different Frame Relay subinterface and Frame Relay DLCI, results in a SIP 200 crash.

  Old Behavior: Installing simultaneous QoS policies on both ATM subinterface and ATM PVC, or on different Frame Relay subinterface and Frame Relay DLCI is allowed.

  New Behavior: Installing simultaneous QoS policies on both ATM subinterface and ATM PVC, or on different Frame Relay subinterface and Frame Relay DLCI is not allowed.
Cisco IOS Release 15.2(4)M3

The following behavior changes are introduced in Cisco IOS Release 15.2(4)M3:

- The “aaa accounting delay-start extended-time” command is introduced to add Framed-IP-Address to the accounting start packets in the dual stack scenario.
  
  Old Behavior: The RADIUS attribute 8 (Framed-IP-Address) is not included in the accounting start packets in the following two scenarios:
  
  - The user is a dual-stack (IPv4 or IPv6) subscriber.
  - The IP address is from a local pool and not from the RADIUS server.
  
  New Behavior: The “aaa accounting delay-start extended-time” command is introduced to delay the accounting start records for the configured time (in seconds) after the IPCPv6 address is sent to the RADIUS server. During this configured delay time, the IPCPv4 address is sent and the Framed-IPv4-Address is added to the accounting start record. If the IPCPv4 address is not sent in the configured delay time, the accounting start record is sent without the Framed-IPv4-Address.

  Additional Information:
  

- The NHRP syslog error message includes the IP address of the node where the error originates.
  
  Old Behavior: The NHRP syslog error message does not include the IP address of the node where the error originates, the source NBMA, and the destination address.
  
  New Behavior: The NHRP syslog error message includes the IP address of the node where the error originates, the source NBMA, and the destination address.

  Additional Information:
  

- Initial INVITE with 0.0.0.0 call flow is supported.
  
  Old Behavior: Initial INVITE with 0.0.0.0 is not supported unless ACK contains valid IP address.
  
  New Behavior: This call flow is supported.

  Additional Information:
  

- Transmission of IPsec Dummy Packets per RFC 4303.
  
  Old Behavior: IOS devices does not conform to RFC 4303.
  
  New Behavior: IOS devices conforms to RFC 4303 to enable transmitting dummy packets.

  Additional Information:
  

- IPv6 support is added for legacy Control Plane Policing (CoPP) on Cisco Express forwarding interfaces.
Old Behavior: IPv6 support is not available for CoPP, resulting in a failure of policing and rate limiting.

New Behavior: IPv6 support is added for legacy CoPP on Cisco Express forwarding interfaces that support aggregate-scope policing and rate limiting.

- The extended keyword is added to the show waas status command.

Old Behavior: The show waas status command displays the status of Wide Area Application Services (WAAS) Express.

New Behavior: The extended keyword is added to the show waas status command. The extended keyword provides complete information for WAAS Express.

Additional Information:

Cisco IOS Release 15.2(4)M2

The following behavior changes are introduced in Cisco IOS Release 15.2(4)M2:

- The show aaa servers command output displays estimated outstanding/throttled access/accounting transactions.

Old Behavior: Outstanding access transactions are left unprocessed on RADIUS server.

New Behavior: The show aaa servers command output displays the number of access, authorization, and accounting requests and estimated outstanding/throttled access/accounting transactions that are being processed. The clear aaa counters servers all command clears all counters except estimated outstanding/throttled access/accounting transactions. These values will automatically reduce.

Additional Information:

- Up to ten classless static routes are supported using option 121 on dhcp client.

Old Behavior: Only two classless static routes were supported using option 121 on the dhcp client.

New behavior: Up to ten classless static routes are supported using option 121 on dhcp client.

Additional Information:

- The advanced protocol pack is provided as the base protocol pack version with a licensed Cisco image.

Old Behavior: A default protocol pack was provided as the base protocol pack version with a Cisco image.

New Behavior: Default protocol packs are no longer supported. The advanced protocol pack is provided as the base protocol pack with a licensed Cisco image on a device. The advanced protocol pack has the complete set of Protocol Description Language files (PDLs) available for a release. The standard protocol pack is provided as the base protocol pack with an unlicensed Cisco image.
Additional Information:


Old Behavior: No restriction on the NAME field for loading an Advanced or Standard Protocol Pack.

Additional information:

- BGP Processing of the Removal of Private AS Numbers from AS Path.

Old Behavior: When the `neighbor remove-private-as` command is configured and a route-map without a continue clause is configured, the processing order is:

1. `neighbor remove-private-as` processing.
2. `set as-path prepend` or `set as-path prepend last-as`.

However, if the route-map contains a continue clause, the processing order is reversed.

New Behavior: When the `neighbor remove-private-as` command is configured and a route-map is configured (whether it has a continue clause or not), the processing order is always:

1. `neighbor remove-private-as` processing.
2. `set as-path prepend` or `set as-path prepend last-as`.

- Metadata service functionality is added to the SAF feature.

Old Behavior: Metadata service functionality is not available.

New Behavior: The Cisco SAF Forwarder can send service metadata to its neighbor SAF nodes. Metadata is XML information, and service data is information that a server communicates to a client about itself. The service metadata does not propagate in mixed 15.1(3)S and 15.2(1)S environments until such time that the version of EIGRP and SAF is upgraded.

Additional Information:

- Default change.

Old Behavior: Earlier, the 7600 platform, on GRE tunnels protected with IPsec and static VTI tunnels, required the configuration of lesser “ip mtu” explicitly on the tunnel interface to prevent fragmentation post encryption.

New Behavior: By default, all overheads including GRE and IPsec are accounted beforehand and the resultant value (i.e. Transport MTU - overhead [GRE+IPsec]) is programmed as ip mtu on these tunnels.

Additional Information:

- The default mode for the default transform set is changed to tunnel.

Old Behavior: The default mode for all transform sets, including the default transform set, is tunnel.
New Behavior: The default mode for the default transform set is transport; the default mode for all other transform sets is tunnel.

Additional Information:

• Cable detection is extended to analog FXS, FXSG, and FXOGS voice ports.

Old Behavior: Cable detection existed on analog FXOLS voice port only.

New Behavior: Cable detection is extended to analog FXS, FXSG, and FXOGS voice ports, and a new CLI cable-detect-poll-timer is introduced to configure the cable polling timer value for background polling processes.


• IKEv2 default max in-negotiation CAC counter has been modified to 40.

Old Behavior: IKEv2 default max in-neg CAC counter was 1000.

New Behavior: IKEv2 default max in-neg CAC counter has been modified to 40 and is true for all platforms.


• Missing threshold for logout calls in the queue display.

Old Behavior: The threshold is missing for logout calls in the queue display. The CLI is hunt-group logout [DND | HLog].

New Behavior: The notify keyword and threshold-number argument are added in the hunt-group logout command to enable the indication of the calls in queue for logout agents using the Hlog Programmable Line Key:

hunt-group logout [DND | HLog | notify | threshold-number]

• Unable to lock out the background settings using the xml append file. Users cannot configure commonProfile xml content and comprise it with the callLogBlfEnabled enabled by “presence call-list”.

Old Behavior: Users cannot configure the commonProfile xml content.

New Behavior: Introduced the following new CLI to set parameters under commonProfile section in IP phone SEP*.cnf.xml configuration files:

service profile [phonePassword password | callLogBlfEnabled | backgroundImageAccess false]

• Monitor pcm-trace profile CLI extended to include analog and BRI voice ports.

Old Behavior: Configuring monitor pcm-trace profile to perform ds0 dumps for analog and BRI voice ports was not possible.

New Behavior: Monitor pcm-trace profile CLI extended to allow dsO dumps to be configured for analog and BRI voice ports.
Additional Information:

- WebEx data, streaming, video, and voice application types are not supported.
  
  Old Behavior: The `webex-data`, `webex-streaming`, `webex-video`, and `webex-voice` keywords are available in the `match application` command.

  New Behavior: The `webex-data`, `webex-streaming`, `webex-video`, and `webex-voice` keywords are not available in the `match application` command.

  Additional Information:  

- Setting of factory defaults.
  
  Old Behavior: When push button is pressed, configuration and image recovery will take place at WLAN AP running on 2nd core of next generation c8xx platforms.

  New Behavior: When push button is pressed, ONLY configuration recovery will take place at WLAN AP running on 2nd core of next generation c8xx platforms.
Features and Important Notes for Cisco IOS Release 15.2(3)T

Contents

These release notes describe the following topics:

- New and Changed Information, page 33
- Important Notes, page 42

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.2M&T and contains the following subsections:

- New Hardware Features Supported in Cisco IOS Release 15.2(3)T3, page 33
- New Hardware Features Supported in Cisco IOS Release 15.2(3)T4, page 34
- New Software Features Supported in Cisco IOS Release 15.2(3)T3, page 34
- New Hardware Features Supported in Cisco IOS Release 15.2(3)T2, page 34
- New Software Features Supported in Cisco IOS Release 15.2(3)T2, page 34
- New Hardware Features Supported in Cisco IOS Release 15.2(3)T1, page 34
- New Software Features Supported in Cisco IOS Release 15.2(3)T1, page 34
- New Hardware Features Supported in Cisco IOS Release 15.2(3)T, page 34
- New Software Features Supported in Cisco IOS Release 15.2(3)T, page 35

New Hardware Features Supported in Cisco IOS Release 15.2(3)T3

A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://www.cisco.com/go/cfn.
New Hardware Features Supported in Cisco IOS Release 15.2(3)T

There are no new hardware features in Cisco IOS Release 15.2(3)T.

New Software Features Supported in Cisco IOS Release 15.2(3)T

There are no new software features in Cisco IOS Release 15.2(3)T.

New Hardware Features Supported in Cisco IOS Release 15.2(3)T2

There are no new hardware features in Cisco IOS Release 15.2(3)T2.

New Software Features Supported in Cisco IOS Release 15.2(3)T2

There are no new software features in Cisco IOS Release 15.2(3)T2.

New Hardware Features Supported in Cisco IOS Release 15.2(3)T1

There are no new hardware features in Cisco IOS Release 15.2(3)T1.

New Software Features Supported in Cisco IOS Release 15.2(3)T1

There are no new software features in Cisco IOS Release 15.2(3)T1.

New Hardware Features Supported in Cisco IOS Release 15.2(3)T

This section describes new and changed features in Cisco IOS Release 15.2(3)T. Some features may be new to Cisco IOS Release 15.2(3)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(3)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

GRWIC Adaptor Card

For detailed information about this feature, see the following documents:

New Software Features Supported in Cisco IOS Release 15.2(3)T

This section describes new and changed features in Cisco IOS Release 15.2(3)T. Some features may be new to Cisco IOS Release 15.2(3)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(3)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

AAA-Domain Stripping at Server Group Level

For detailed information about this feature, see the following document:

Add New Media Quality MIBs Support

Voice quality statistics are collected on ISR platforms to provide useful data regarding voice transmission and reception quality. New Acoustic Shock Protection (ASP) and Noise Reduction (NR) statistics, among many other voice and video quality metrics, are included in a Management Information Base (MIB) object called CISCO-MEDIA-QUALITY-MIB. This MIB can be used for MIB-based Simple Network Management Protocol (SNMP) polling and management. These media quality statistics are presented in Object Identification (OID) format.

ASP/NR

For detailed information about this feature, see the following documents:

BGP Best External

For detailed information about this feature, see the following documents:

BGP Diverse Path Using Diverse-Path-RR

For detailed information about this feature, see the following document:
New and Changed Information

BGP IPv6 Client for Single Hop BFD

For detailed information about this feature, see the following documents:

BGP IPv6 PIC Edge and Core for IP/MPLS

For detailed information about this feature, see the following documents:

BGP PIC Edge for IP/MPLS

For detailed information about this feature, see the following documents:

BGP Route Server

For detailed information about this feature, see the following document:

BGP—RT Constrained Route Distribution

For detailed information about this feature, see the following document:

CAC for IPv6 Flows

For detailed information about this feature, see the following document:

Cisco-BGP-MIBv2

For detailed information about this feature, see the following document:

Cisco IOS Zone-Based Policy Firewall High Availability

For detailed information about this feature, see the following document:
Dying Gasp Support for Loss of Power Supply via SNMP, Syslog and Ethernet OAM

For detailed information about this feature, see the following document:

EIGRP Dual DMVPN Domain Enhancement

For detailed information about this feature, see the following document:

Extensible Messaging Client Protocol (XMCP) 2.0

For detailed information about this feature, see the following document:

GET VPN Support for IPv6 in the Data Plane

For detailed information about this feature, see the following document:

GRWIC Adaptor Card

For detailed information about this feature, see the following documents:

IEEE 802.1ab Link Layer Discovery Protocol (LLDP)

For detailed information about this feature, see the following document:

IEEE 802.1ab LLDP Local and Remote System MIBs

Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on a local network. A network management system can model the topology of the network by querying MIB databases in the devices. The maximum number of neighbor entries that LLDP supports is 12000. The maximum number of management addresses per station is 10. When LLDP is supported, the IEEE 802.1ab LLDP Local and Remote Systems MIB (IEEE 802.1ab LLDP MIB) is also supported.
Two sub-MIBs, the local system MIB and remote systems MIB, make up the IEEE 802.1ab LLDP MIB. The LLDP local system sub-MIB must be included on all platforms where transmission capability can be enabled. The LLDP remote systems sub-MIB is required where receipt of LLDP frames can be enabled.

The IEEE 802.1ab LLDP MIB interacts with the IF MIB to get network information and with the LLDP to obtain local and remote system information. When the Simple Network Management Protocol (SNMP) receives requests from the SNMP manager station and sends getmany queries, the IEEE 802.1ab LLDP MIB provides the requested information.

To use the IEEE 802.1ab LLDP MIB, LLDP must be configured and the IF MIB must be present. Users interact with the IEEE 802.1ab LLDP MIB using the SNMP manager application. The CLI command `snmp-server community public ro` or a similar command is required to enable the SNMP agent. Otherwise, no particular commands or configuration settings are required to use the IEEE 802.1ab LLDP MIB.


For detailed information about the IEEE 802.1ab LLDP MIB, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at http://www.cisco.com/go/mibs.

**Inter-Chassis Asymmetric Routing Support on Zone-Based Firewall**

For detailed information about this feature, see the following document:


**IP SLAs TWAMP Responder v1.0**

For detailed information about this feature, see the following document:


**IPSLA 4.0—IPv6 Phase2**

For detailed information about this feature, see the following documents:

IPv6 ACL Extensions for Hop by Hop Filtering

For detailed information about this feature, see the following document:

IPv6 Remote Access for IPSec VPN

For detailed information about this feature, see the following document:

LISP PETR Load Sharing

The LISP PETR Load Sharing feature adds priority and weight options to configured PETRs for configurable load sharing. For detailed information about this feature, see the following document:

LISP Route-Import

The LISP Route-Import feature enables dynamic proxying of EID-space by a Proxy-ITR. For detailed information about this feature, see the following document:

LISP Virtualization Support for Multiple Parallel RLOC Domains

For detailed information about this feature, see the following document:

LLDP IPv6 Address Support

Cisco IOS Release 15.2(3)T and later releases support IPv6 Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (MED) addresses.
New and Changed Information

Media Services Proxy Functionality on T-train for ISR-G2
For detailed information about this feature, see the following document:

MediaTrace 2.0
For detailed information about this feature, see the following document:

MoFRR
For detailed information about this feature, see the following document:

Multicast Live-Live
For detailed information about this feature, see the following document:

Multicast Service Reflection
For detailed information about this feature, see the following document:

NTPv4 Orphan Mode Support, Range for Trusted Key Configuration
For detailed information about this feature, see the following document:

OSPFv3 External Path Preference Option (RFC 5340 from RFC 2328 16.4.1)
For detailed information about this feature, see the following document:

OSPFv3 Max-Metric Router-LSA
For detailed information about this feature, see the following document:

Performance Monitor Metadata Support
For detailed information about this feature, see the following document:

**PfR Auto Discovery v1.0**

For detailed information about this feature, see the following document:

**PfR BR Auto Neighbors**

For detailed information about this feature, see the following document:

**PfR BR Automatic Adjacencies**

For detailed information about this feature, see the following document:

**PIMv6—Anycast RP Solution**

For detailed information about this feature, see the following document:

**RSVP Multicast CAC**

For detailed information about this feature, see the following document:

**RTP Port Range**

For ASR boxes, the RTP port range has been increased to a range of 8000 to 48200 to scale high call volumes. This port range allows up 10000 calls on a single interface.
For detailed information about this feature, see the following document:
#task_39847922DDE9413BAFE73A80EE44EA5D

**Service Module IPv6 Gateway Support**

For detailed information about this feature, see the following document:
Support CEF Switching of IPv6 Traffic on Dialer Interfaces
For detailed information about this feature, see the following document:

Support Multiple xTRs with Dynamic RLOCs at a Site
For detailed information about this feature, see the following document:

VLAN 0 Priority Tagging Support
For detailed information about this feature, see the following documents:

WAAS Express Phase 2
For detailed information about this feature, see the following documents:

WCCP—Configurable Router ID
For detailed information about this feature, see the following documents:

WCCP—Fast Timers
For detailed information about this feature, see the following documents:

WCCPv2—IPv6 Support
For detailed information about this feature, see the following documents:

Important Notes
The following information applies to all releases of Cisco IOS Release 15.2T.
- Cisco IOS Behavior Changes, page 43
- Field Notices and Software-Related Tools and Information, page 46
Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

Behavior changes are provided for the following releases:

- Cisco IOS Release 15.2(3)T3, page 43
- Cisco IOS Release 15.2(3)T2, page 44
- Cisco IOS Release 15.2(3)T1, page 45

Cisco IOS Release 15.2(3)T3

The following behavior changes are introduced in Cisco IOS Release 15.2(3)T3:

- Virtual template lock functionality change.
  Old Behavior: A virtual template of the type tunnel with cloned virtual access interfaces can be configured. The virtual template dynamically updates the configuration to the cloned virtual access interfaces, thereby causing instability in some scenarios.
  New Behavior: A virtual template of the type tunnel having with cloned virtual access interfaces cannot be configured.
  Additional Information:

- The default mode for the default transform set is changed to tunnel.
  Old Behavior: The default mode for all transform sets, including the default transform set, is tunnel.
  New Behavior: The default mode for the default transform set is transport; the default mode for all other transform sets is tunnel.
  Additional Information:

- Initial INVITE with 0.0.0.0 call flow is supported.
  Old Behavior: Initial INVITE with 0.0.0.0 is not supported unless ACK contains valid ip address.
  New Behavior: This call flow is supported.
  Additional Information:
Cisco IOS Release 15.2(3)T2

The following behavior changes are introduced in Cisco IOS Release 15.2(3)T2:

- Up to ten classless static routes are supported using option 121 on the DHCP client.
  
  Old Behavior: Only two classless static routes were supported using option 121 on the DHCP client.
  
  New Behavior: Up to ten classless static routes are supported using option 121 on the DHCP client.
  
  Additional Information:
  [Link to Cisco documentation]

- BGP processing of the removal of private AS numbers from the AS path.
  
  Old Behavior: When the neighbor remove-private-as command is configured and a route-map without a continue clause is configured, the processing order is:
  
  1. neighbor remove-private-as processing
  2. set as-path prepend or set as-path prepend last-as
  
  However, if the route-map contains a continue clause, the processing order is reversed.
  
  New Behavior: When the neighbor remove-private-as command is configured and a route-map is configured (whether it has a continue clause or not), the processing order is always:
  
  1. neighbor remove-private-as processing
  2. set as-path prepend or set as-path prepend last-as

- Virtual template lock functionality.
  
  Old Behavior: A virtual template of the type tunnel with cloned virtual access interfaces can be configured. The virtual template dynamically updates the configuration to the cloned virtual access interfaces, thereby causing instability in some scenarios.
  
  New Behavior: A virtual template of the type tunnel having with cloned virtual access interfaces cannot be configured.
  
  Additional Information:
  [Link to Cisco documentation]

- In the IPsec SVTI configuration with HA, existing security associations are not affected.
  
  Old Behavior: When configuring IPsec SVTI with HA, the standby router reload interrupts the existing security associations.
  
  New Behavior: When configuring IPsec SVTI with HA, the standby router reload does not affect the existing security associations.
  
  Additional Information:
  [Link to Cisco documentation]

- HLog PLK blinks, the hunt member logs out, and the conference call is blocked.
  
  Old Behavior: There is no label configuration for the feature button.
  
  New behavior: There is label configuration for feature buttons.
  
  Additional Information:
  [Link to Cisco documentation]

- IKEv2 default max in-negotiation CAC counter has been modified to 40.
  Old Behavior: IKEv2 default max in-neg CAC counter is 1000.
  New Behavior: IKEv2 default max in-neg CAC counter has been modified to 40 and is true for all platforms.

- Missing threshold for logout calls in the queue display.
  Old Behavior: The threshold is missing for logout calls in the queue display. The CLI is `hunt-group logout [DND | HLog].`
  New Behavior: The `notify` keyword and `threshold-number` argument are added in the `hunt-group logout` command to enable the indication of the calls in queue for logout agents using the Hlog Programmable Line Key.

```
hunt-group logout [DND | HLog | notify | threshold-number]
```

- Unable to lock out the background settings using the xml append file. Users cannot configure commonProfile xml content and comprise it with the callLogBlfEnabled enabled by “presence call-list”.
  Old Behavior: Users cannot configure the commonProfile xml content.
  New Behavior: Introduced the following new CLI to set parameters under commonProfile section in IP phone SEP*.cnf.xml configuration files.

```
service profile [phonePassword password | callLogBlfEnabled | backgroundImageAccess false]
```

- The `clear call threshold interface` command can be used for a Gigabit Ethernet interface.
  Old Behavior: Unable to the `clear call threshold interface` command for a Gigabit Ethernet interface.
  New Behavior: Gigabit Ethernet interface is a valid interface type.

- WebEx data, streaming, video, and voice application types are not supported.
  Old Behavior: The `webex-data`, `webex-streaming`, `webex-video`, and `webex-voice` keywords are available in the `match application` command.
  New Behavior: The `webex-data`, `webex-streaming`, `webex-video`, and `webex-voice` keywords are not available in the `match application` command.

**Cisco IOS Release 15.2(3)T1**

The following behavior changes are introduced in Cisco IOS Release 15.2(3)T1:

- Configure “radius-server attribute 44 include-in-access-req all” instead of “radius-server attribute 44 include-in-access-req” if the per VRF-level attribute inclusion is not required.
Old Behavior: The `radius-server attribute 44 include-in-access-req` command applies attribute 44 for all the sessions.

New Behavior: The command is modified to include the configuration of non-VRF sessions.

Additional Information: 

・ When ATM subinterfaces need to be assigned an IP address from a DHCP server, the MAC address on the main interface can be reused for the subinterface.

Old Behavior: The MAC address configured by the `atm ether-mac-address` command could not be reused for the subinterface.

New Behavior: The MAC address configured by the `atm ether-mac-address` command can be reused using the `reuse-mac` keyword.

```
ip dhcp client client-id {interface-name | ascii string | hex string}
```

New Behavior: The MAC address configured by the `atm ether-mac-address` command can be reused using the `reuse-mac` keyword.

```
ip dhcp client client-id {interface-name | ascii string | hex string | reuse-mac}
```

Additional Information: 

・ Change to how IPv6 paths are advertised.

Old Behavior: An IPv6 path is advertised without a label when the label has not been negotiated.

New Behavior: IPv6 paths are not advertised if the label has not been negotiated.

・ The `mode tunnels` command is disabled by default.

Old Behavior: PfR automatically creates dynamic tunnels between all border routers.

New Behavior: Dynamic tunnels are not automatically created between border routers.

Additional Information: 

・ For the Carrier Packet Transport (CPT) system, an alert is displayed whenever a round-trip delay threshold violation occurs during an IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation.

Old Behavior: When a round-trip delay exceeds the specified threshold, an event is sent and IP SLAs generate a notification to the network management application.

New Behavior: For the CPT system, when a round-trip delay threshold violation occurs during an IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation, an alert is displayed, in addition to IP SLAs sending a notification. The alert is cleared when the round-trip delay falls back below the specified threshold value.

Additional Information: 

**Field Notices and Software-Related Tools and Information**

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at 

Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at 
Features and Important Notes for Cisco IOS Release 15.2(2)T

Contents

These release notes describe the following topics:

- New and Changed Information, page 47
- Important Notes, page 56

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.2M&T and contains the following subsections:

- New Hardware Features Supported in Cisco IOS Release 15.2(2)T, page 47
- New Software Features Supported in Cisco IOS Release 15.2(2)T, page 48

Note

A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://www.cisco.com/go/cfn.

New Hardware Features Supported in Cisco IOS Release 15.2(2)T

This section describes new and changed features in Cisco IOS Release 15.2(2)T. Some features may be new to Cisco IOS Release 15.2(2)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(2)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.
**New and Changed Information**

**New and Changed Information**

**Cisco 860 Series Integrated Services Routers**

Cisco IOS Release 15.2(2)T will provide support for the Cisco 860VAE Integrated Services Router Generation 2. The Cisco 860VAE is ideal for deployments into small offices or service provider-managed CPEs. The Cisco 860VAE is flexible, silent, compact, and cost optimized. The Cisco 860VAE provides multiple WAN options for maximum deployment flexibility along with optional market leading features such as ScanSafe connector, BGP, IPSec and firewall. The Cisco 860VAE series ISR is available as a base router with an IPBase IOS image or a secure router with an advanced security IOS image with or without payload encryption.

**G.SHDSL EFM/ATM Multimode**

For detailed information about this feature, see the following document:


**SM-32A Module Support on ISR G2 3900/3900E Platforms**

For detailed information about this feature, see the following document:


**New Software Features Supported in Cisco IOS Release 15.2(2)T**

This section describes new and changed features in Cisco IOS Release 15.2(2)T. Some features may be new to Cisco IOS Release 15.2(2)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(2)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

**802.1Q Tunneling (QnQ) and Layer 2 Protocol Tunneling (L2PT) Support on ISR G2**

For detailed information about this feature, see the following document:


**Add New Media Quality MIBs Support**

Voice quality statistics are collected on ISR platforms to provide useful data regarding voice transmission and reception quality. New Acoustic Shock Protection (ASP) and Noise Reduction (NR) statistics, among many other voice and video quality metrics, are included in a Management Information Base (MIB) object called CISCO-MEDIA-QUALITY-MIB. This MIB can be used for MIB-based Simple Network Management Protocol (SNMP) polling and management. These media quality statistics are presented in Object Identification (OID) format.
AS SIP—DSCP Policing

For detailed information about this feature, see the following document:


AS SIP—Media Bandwidth Policing

For detailed information about this feature, see the following document:


ASP/NR

For detailed information about this feature, see the following documents:


Audio/Video RTCP Passthru on ISR Gateways for MTP, TRP, RSVPAgent Services

For detailed information about this feature, see the following document:


Bandwidth-based Call Admission Control (CAC)

For detailed information about this feature, see the following document:


Call Rate CLI

For detailed information about this feature, see the following document:


Callhome V2 Enhancements

For detailed information about this feature, see the following document:


Capabilities Manager

For detailed information about this feature, see the following document:

New and Changed Information

CDP Enhancement—Host Presence TLV

For detailed information about this feature, see the following document:


CME 9.0

For detailed information about this feature, see the following documents:


Connected Grid Swap Drive—CGR 2010

For detailed information about this feature, see the following document:


Critical VLAN with Multi-Auth

For detailed information about this feature, see the following document:


Critical Voice VLAN Support

For detailed information about this feature, see the following document:


DMVPN—NHRP Event Publisher

For detailed information about this feature, see the following document:


Egress DSCP Marking for GRE Tunnels

For detailed information about this feature, see the following document:


Embedded Event Manager (EEM) 4.0

For detailed information about this feature, see the following document:

**Flexible NetFlow: Export to an IPv6 Address**

For detailed information about this feature, see the following documents:

**FlexVPN Spoke to Spoke**

For detailed information about this feature, see the following document:

**Handle Multiple Early Dialog Messages**

For detailed information about this feature, see the following document:

**IEEE 802.1X—Auth Fail VLAN**

For detailed information about this feature, see the following document:

**IEEE 802.1X with ACL Assignments**

For detailed information about this feature, see the following document:

**IEEE 802.1X Authenticator**

For detailed information about this feature, see the following document:

**IEEE 802.1X—Common Session ID**

For detailed information about this feature, see the following document:
IEEE 802.1X—Conditional Logging

For detailed information about this feature, see the following document:


IEEE 802.1X—Flexible Authentication

For detailed information about this feature, see the following document:


IEEE 802.1X Guest VLAN

For detailed information about this feature, see the following document:


IEEE 802.1X Multi-Domain Authentication

For detailed information about this feature, see the following document:


IEEE 802.1X—Multiple Authentication

For detailed information about this feature, see the following document:


IEEE 802.1X—Open Authentication

For detailed information about this feature, see the following document:


IEEE 802.1X—RADIUS Change of Authorization (CoA)

For detailed information about this feature, see the following document:


IEEE 802.1X—Wake on LAN Support

For detailed information about this feature, see the following document:

IP SLAs Video Operation

For detailed information about this feature, see the following document:

IPv6 Compliance of Cisco IPSec MIBs and IKEv2 Extensions to Cisco IPSec MIB

For detailed information about this feature, see the following document:

IPv6 Support for NBAR

The IPv6 Support for NBAR feature introduces the `ip nbar classification tunneled-traffic` command to enable application classification of IPv6 traffic carried over IPv4 tunnels in Network Based Application Recognition (NBAR).

ISDN UDI to SIP Clear-Channel

For detailed information about this feature, see the following document:

LISP Instance ID Support

The LISP Instance ID Support feature includes the following support:

- Single-tenancy support on xTR: Ability to associate an instance ID to a single LISP instance running on an xTR. This allows for xTRs that are connected to the same network to use different LISP instances resulting in segmentation of the EID prefixes that they support.
- Multi-tenancy support on MS/MR: Ability for an MS/MR to maintain segmentation of the EID prefixes between instance IDs when providing mapping services to xTRs that are running with different LISP instance IDs.

Multi-Auth VLAN Assignment

Support for VLAN assignment on a port configured for multi-auth mode. The RADIUS server assigns a VLAN to the first host to authenticate on the port, and subsequent hosts use the same VLAN. Voice VLAN assignment is supported for one IP phone.

NAT Aware RSVP

For detailed information about this feature, see the following document:
New and Changed Information

NBAR Categorization and Attributes

For detailed information about this feature, see the following document:

NBAR PDL Supported in PI17

For detailed information about this feature, see the following document:

NBAR Protocol Pack

For detailed information about this feature, see the following document:

NEAT (Network Edge Authentication Topology)

For detailed information about this feature, see the following document:

Open API for IOS UC Services

For detailed information about this feature, see the following document:

OSPF Support for NSSA RFC 3101

For detailed information about this feature, see the following document:

Performance Monitor (Phase 2)

For detailed information about this feature, see the following document:

Per-User ACL Support for 802.1X/MAB/Webauth Users

For detailed information about this feature, see the following document:
PfR Data Export v1.0 NetFlow v9 Format

For detailed information about this feature, see the following document:

PfR SNMP MIB v1.0 (Read-Only)

For detailed information about this feature, see the following document:

Standalone MAB Support

For detailed information about this feature, see the following document:

Support for Trustsec Solution on ISR Platforms

For detailed information about this feature, see the following document:

TrustSec—Secure Group Tag (SGT), Secure Exchange Protocol (SXP) over TCP (SXPoTCP), Secure Group Firewall (SGFW) Using Zone-Based Firewall (ZBFW)

For detailed information about this feature, see the following document:

Video Monitoring MIB Support for Medianet Video Monitoring

This feature provides support for the use of the industry-standard Simple Network Management Protocol (SNMP) to monitor media streams. This support is implemented with the addition of the following Cisco proprietary SNMP Management Information Base (MIB) modules:

- CISCO-FLOW-MONITOR-TC-MIB—Defines the textual conventions common to the following MIB modules.
- CISCO-FLOW-MONITOR-MIB—Defines the framework that describes the flow monitors supported by a system, the flows that it has learned, and the flow metrics collected for those flows.
- CISCO-MDI-METRICS-MIB—Defines objects that describe the quality metrics collected for media streams that comply to the Media Delivery Index (MDI) [RFC 4445].
- CISCO-RTP-METRICS-MIB—Defines objects that describe the quality metrics collected for RTP streams, similar to those described by an RTCP Receiver Report packet [RFC 3550].
- CISCO-IP-CBR-METRICS-MIB—Defines objects that describe the quality metrics collected for IP streams that have a Constant Bit Rate (CBR).
For detailed information about these MIBs, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at http://www.cisco.com/go/mibs. This feature also includes two new command-line interface (CLI) commands and one modified CLI command. The commands are as follows:

- `snmp-server host`—Enables the delivery of flow monitoring SNMP notifications to a recipient.
- `snmp-server enable traps flowmon`—Enables flow monitoring SNMP notifications. By default, flow monitoring SNMP notifications are disabled.
- `snmp mib flowmon alarm history`—Sets the maximum number of entries maintained by the flow monitor alarm history log.

For more information about these commands, see the Cisco IOS Master Command List.

**Web Authentication with Critical Auth Support**

For detailed information about this feature, see the following document:


**Webauth Enhancements**

For detailed information about this feature, see the following document:


We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at http://www.cisco.com/cisco/web/download/index.html.

**Important Notes**

The following information applies to all releases of Cisco IOS Release 15.2T.

- Cisco IOS Behavior Changes, page 56
- Field Notices and Software-Related Tools and Information, page 62

**Cisco IOS Behavior Changes**

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

Behavior changes are provided for the following releases:
Cisco IOS Release 15.2(2)T4

The following behavior changes are introduced in Cisco IOS Release 15.2(2)T4:

- PfR syslog levels have been added to minimize the number of messages.
  
  Old Behavior: Too many PfR syslog messages are generated.
  
  New Behavior: PfR syslog levels has been added to minimize the number of messages displayed and a syslog notice has been added to display when 30 percent of the traffic classes are out-of-policy.
  

- IPv6 support is added for legacy Control Plane Policing (CoPP) on Cisco Express forwarding interfaces.
  
  Old Behavior: IPv6 support is not available for CoPP, resulting in a failure of policing and rate limiting.
  
  New Behavior: IPv6 support is added for legacy CoPP on Cisco Express forwarding interfaces that supports aggregate-scope policing and rate limiting.

Cisco IOS Release 15.2(2)T3

The following behavior changes are introduced in Cisco IOS Release 15.2(2)T3:

- BGP Processing of the Removal of Private AS Numbers from AS Path.
  
  Old Behavior: When the neighbor remove-private-as command is configured and a route-map without a continue clause is configured, the processing order is:
  
  1. neighbor remove-private-as processing.
  2. set as-path prepend or set as-path prepend last-as.
  
  However, if the route-map contains a continue clause, the processing order is reversed.
  
  New Behavior: When the neighbor remove-private-as command is configured and a route-map is configured (whether it has a continue clause or not), the processing order is always:
  
  1. neighbor remove-private-as processing.
  2. set as-path prepend or set as-path prepend last-as.

- RTP signal processing is disabled by default.
  
  Old Behavior: RTP packets of payload type “123” can cause errors on Cisco AS5350 and AS5400 series platforms.
  
  New Behavior: RTP signal processing is disabled by default to prevent errors caused by RTP packets of payload type “123,” and can be enabled when necessary using the voice-fastpath voice-rtp-signalling enable command.
  
• A CLI “rtp-media-loop count” is introduced to control the maximum loop count before media packets are dropped.

Old Behavior: For IP-IP calls, there was no mechanism to limit the number of possible media loops before the media packets are dropped.

New Behavior: A CLI “rtp-media-loop count” is provisioned globally under voice service voip configuration mode to control the maximum loop count before media packets are dropped.

Additional Information:

Cisco IOS Release 15.2(2)T2

The following behavior changes are introduced in Cisco IOS Release 15.2(2)T2:

• The status of the `snmp trap link-status` command on an ATM subinterface changes when the device is reloaded.

Old Behavior: The `snmp-server enable traps atm subif` command enables Simple Network Management Protocol (SNMP) link trap generation on all the ATM subinterfaces. When the device is reloaded SNMP trap generation is enabled on all ATM subinterfaces.

New Behavior: To enable SNMP link trap generation on an ATM subinterface, first configure the `snmp-server enable traps atm subif` command in global configuration mode and then configure the `snmp trap link-status` command on the ATM subinterface on which SNMP link trap generation is to be enabled.

Additional Information:

• Connected number and Connected name are sent in an ISDN CONNECT message as Connected Number IE and Connected Name (display IE).

Old Behavior: Connected number and Connected name that are signaled to Cisco IOS software from a SIP 200 OK message are not sent in an ISDN CONNECT message.

New Behavior: Connected number and Connected name that are signaled to Cisco IOS software from a SIP 200 OK message are sent as Connected Number IE and Display IE (Connected Name) in the ISDN CONNECT message. Passing the connected number and the connected name is enabled by configuring the following commands in interface configuration mode: `isdn outgoing ie connected-number; isdn outgoing ie display`.

Additional Information:

• Change to how IPv6 paths are advertised.

Old behavior: An IPv6 path is advertised without a label when the label has not been negotiated.

New behavior: IPv6 paths are not advertised if the label has not been negotiated.


• Collected CLI set for the Call Home full inventory message are modified.

Old Behavior: The following show commands are included in the call home full inventory message:
show diag, show version, show inventory oid, show environment all, show license udi, show license all, show interfaces, show file systems, show flash:all, show data-corruption, show
memory statistics, show process memory, show process cpu, show process cpu history, show crypto engine configuration, show crypto engine accelerator statistics, show license detail, show license statistics, show buffers, and show ip nat statistics.

New Behavior: The following show commands are included in the call home full inventory message: show diag, show version, show inventory oid, show environment all, show license udi, show license all, show interfaces, show file systems, show flash:all, show data-corruption, show memory statistics, show process memory sorted, show process cpu sorted, show process cpu history, show license detail, show license statistics, show buffers, show ip route, show access-list, show ip protocols, show ip arp, and show cdp neighbors.

Additional Information:

- A profile in the anonymous mode can send crash messages.

The crash keyword is available in the call-home send alert-group command now. The crash keyword helps send a system crash message with the latest crash information to the destination profile.

Old Behavior: Crash message is not sent when the system crashes and the crash keyword is unavailable in the call-home send alert-group command.

New Behavior: Crash message is sent when the system crashes and the crash keyword is available in the call-home send alert-group command.

Additional Information:

- PfR syslog levels have been added to minimize the number of messages.

Old Behavior: Too many PfR syslog messages are generated.

New Behavior: PfR syslog levels have been added to minimize the number of messages displayed and a syslog notice has been added to display when 30 percent of the traffic classes are out-of-policy.

Additional Information:

- 1. Delta inventory messages are now included in the CLI output for show call-home.

Old Behavior: Delta inventory is not subscribed in CiscoTAC-1 profile.

New Behavior: Delta inventory is subscribed in CiscoTAC-1 profile, allowing OIR event and bootup inventory to be sent to Cisco.

Additional Information:

- 2. A show command is added to inventory messages.

Old Behavior: show ip traffic is not included in inventory messages.

New Behavior: show ip traffic is now included in all types of inventory messages.

Additional Information:

- 3. An inventory message is sent out when call-home reporting command is enabled in anonymous mode.
Old Behavior: An inventory message is not sent out when the call-home reporting command is enabled in anonymous mode, hence Cisco backend servers are not able to show the device report.

New Behavior: If the call-home reporting command causes any change in call-home, an anonymous full inventory message is sent when the configuration finishes. The anonymous inventory message collects the same CLI output as delta inventory message.

Additional Information:

- HLog PLK blinks, hunt member logs out, confcall blocked.

Old behavior: No label configuration for the feature button.

New behavior:
- Modified feature-button command to add label.
- Modified show-ephone hunt command to add members initial state: logout/login.
- Modified ephone-hunt to add members initial state: logout/login.
- Added members logout command.
- Added conference transfer-pattern command.
- Updated Customizing Soft Keys chapter to add label in the “SCCP: Configuring Feature Buttons on a Line Key” section.
- Updated Customizing Soft Keys chapter to add LED table based on Gilera SFS.

Additional information:

- Missing threshold for logout call in queue display. Updated CLI to enable the indication of the calls in queue for logout agents using the Hlog Programmable Line Key.

Old behavior: hunt-group logout [DND | HLog].

New behavior: hunt-group logout [DND | HLog | notify | threshold number]

- Unable to lock out the background settings using xml append file. We need to allow users to configure commonProfile xml content and comprise it with the callLogBlfEnabled enabled by presence call-list. A new CLI service profile is added.

Old behavior: Users cannot configure the commonProfile xml content.

New behavior: Introduced new CLI:

service profile [phonePassword password | callLogBlfEnabled | backgroundImageAccess false]

- Connected number and Connected name are sent in an ISDN CONNECT message as Connected Number IE and Connected Name (display IE).

Old Behavior: Connected number and Connected name that are signaled to Cisco IOS software from a SIP 200 OK message are not sent in an ISDN CONNECT message.

New Behavior: Connected number and Connected name that are signaled to Cisco IOS software from a SIP 200 OK message are sent as Connected Number IE and Display IE (Connected Name) in the ISDN CONNECT message. Passing the connected number and the connected name is enabled by configuring the following commands in interface configuration mode: isdn outgoing ie connected-number, isdn outgoing ie display.

Additional Information:
The clear call threshold interface command can be used for a Gigabit ethernet interface.

Old Behavior: Unable to clear call threshold interface command for a gigabit ethernet interface.
New Behavior: Gigabit ethernet interface is a valid interface type.

Additional Information:

Cisco IOS Release 15.2(2)T1

The following behavior changes are introduced in Cisco IOS Release 15.2(2)T1:

- Change in BGP next-hop for redistributed recursive static routes.
  Old Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be itself. The local next-hop (equal to next-hop-self) is kept.
  New Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be the recursive next-hop of the static route.

- A new keyword is added to the supplementary-service sip command.
  Old Behavior: The handle-replaces keyword is not available in the supplementary-service sip command.
  New Behavior: The handle-replaces keyword is available in the supplementary-service sip command.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr4/vcr-s12.html#GUID-98E8D5E4-A18F-499D-49D4-ACC7-8104E01A0C1A

- New standard and system keywords are added to the existing dtmf-interworking command under voice-service and dial-peer configuration modes.
  Old Behavior: SIP INFO DTMF digit to RFC-4733 DTMF interworking is not supported.
  New Behavior: The newly added standard keyword generates RTP NTE packets that are RFC-4733 compliant.

  Additional Information:

- Added analogue vm-integration in SIP line.
  Old Behavior: vm-integration applies only to SCCP line.
  New Behavior: vm-integration also applies to SIP line.

  Additional Information:

  1. The chapter was updated to apply to both SCCP and SIP.
  2. Added the call-forward b2bua busy and call-forward b2bua noan commands to configure vm-integration for SIP line.
• The IKEv2 profile name must be specified to disassociate it from a crypto map or IPsec profile.
  Old Behavior: The IKEv2 profile name does not need to be specified to disassociate it from a crypto map or IPsec profile.
  New Behavior: The IKEv2 profile name must be specified to disassociate it from a crypto map or IPsec profile.
  Additional Information:

• Fast Network Time Protocol (NTP) synchronization is achieved.
  Old Behavior: The burst and initial burst (iburst) modes are enabled manually.
  New Behavior: The burst and iburst modes are enabled by default.
  Additional Information:

• The **telecom-solutions** keyword is not supported.
  Old Behavior: The **telecom-solutions** keyword in the **ntp refclock** command allows users to configure the reference clock driver.
  New Behavior: Effective with CSCtu20233, the **telecom-solutions** keyword, along with its options, is visible but cannot be configured.
  Additional Information:

---

**Field Notices and Software-Related Tools and Information**

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at http://www.cisco.com/cisco/web/download/index.html.
Features and Important Notes for Cisco IOS Release 15.2(1)T

Contents

These release notes describe the following topics:

- New and Changed Information, page 63
- Important Notes, page 72

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.2(1)T and contains the following subsections:

- New Hardware Features Supported in Cisco IOS Release 15.2(1)T4, page 64
- New Software Features Supported in Cisco IOS Release 15.2(1)T4, page 64
- New Hardware Features Supported in Cisco IOS Release 15.2(1)T3, page 64
- New Software Features Supported in Cisco IOS Release 15.2(1)T3, page 64
- New Hardware Features Supported in Cisco IOS Release 15.2(1)T2, page 64
- New Software Features Supported in Cisco IOS Release 15.2(1)T2, page 64
- New Hardware Features Supported in Cisco IOS Release 15.2(1)T1, page 64
- New Software Features Supported in Cisco IOS Release 15.2(1)T1, page 65
- New Hardware Features Supported in Cisco IOS Release 15.2(1)T, page 65
- New Software Features Supported in Cisco IOS Release 15.2(1)T, page 66

Note

A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://www.cisco.com/go/cfn.
New Hardware Features Supported in Cisco IOS Release 15.2(1)T4

There are no new hardware features in Cisco IOS Release 15.2(1)T4.

New Software Features Supported in Cisco IOS Release 15.2(1)T4

There are no new software features in Cisco IOS Release 15.2(1)T4.

New Hardware Features Supported in Cisco IOS Release 15.2(1)T3

There are no new hardware features in Cisco IOS Release 15.2(1)T3.

New Software Features Supported in Cisco IOS Release 15.2(1)T3

There are no new software features in Cisco IOS Release 15.2(1)T3.

New Hardware Features Supported in Cisco IOS Release 15.2(1)T2

There are no new hardware features in Cisco IOS Release 15.2(1)T2.

New Software Features Supported in Cisco IOS Release 15.2(1)T2

There are no new software features in Cisco IOS Release 15.2(1)T2.

New Hardware Features Supported in Cisco IOS Release 15.2(1)T1

This section describes new and changed features in Cisco IOS Release 15.2(1)T1. Some features may be new to Cisco IOS Release 15.2(1)T1 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(1)T1. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

VPN Acceleration Module (ISM-VPN/SSL) for ISR G2 Routers

For detailed information about this feature, see the following documents:

New Software Features Supported in Cisco IOS Release 15.2(1)T1

This section describes new and changed features in Cisco IOS Release 15.2(1)T1. Some features may be new to Cisco IOS Release 15.2(1)T1 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(1)T1. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

ScanSafe Web Security

For detailed information about this feature, see the following document:

Note
Cisco ISR Web Security with Cisco ScanSafe support in Cisco IOS 15.2(1)T1 will not support User Authentication NTLM (Passive/Explicit), Web Auth Proxy, and HTTP Basic.

New Hardware Features Supported in Cisco IOS Release 15.2(1)T

This section describes new and changed features in Cisco IOS Release 15.2(1)T. Some features may be new to Cisco IOS Release 15.2(1)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(1)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

EHWIC Multimode VDSL2/ADSL+

For detailed information about this feature, see the following documents:
**Multi-Mode 4G LTE for ISR G2**

Cisco EHWIC-4G-LTEs are single-wide EHWICs supported on Cisco 1900 series, 2900 series, and 3900 series integrated services routers generation 2 (ISR G2). They operate over fourth generation (4G) long-term evolution (LTE) cellular networks and third generation (3G) cellular networks.

**New Software Features Supported in Cisco IOS Release 15.2(1)T**

This section describes new and changed features in Cisco IOS Release 15.2(1)T. Some features may be new to Cisco IOS Release 15.2(1)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.2(1)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

**ADSL2/2+ Annex M Mode over POTS VDSL2/ADSL Multimode Annex A SKUs**

Cisco IOS Release 15.2(1)T adds support for enabling Annex M data structures on Cisco 887VA platforms and Annex A data structures on Cisco 887VA-M platforms. This feature allows both Annex A and Annex M structures to be run on the same platform with a performance trade-off for the annex that is not optimized for the device. With this feature implementation, the modes supported on Annex A platforms will be the same as the modes supported on Annex M platforms (887VA-M and EHWIC-1DSL-VA-M). When digital subscriber line access multiplexer (DSLAM) supports Annex M, Annex M mode takes precedence over Annex A mode.

**Cisco UBE Mid-call Re-INVITE Consumption**

For detailed information about this feature, see the following document:


**Cisco UBE RTCP Voice Pass-Through for IPv6**

For detailed information about this feature, see the following document:


**Cisco UBE SNMP MIBs**

The Cisco UBE SNMP MIB feature provides the capability for managing and monitoring the Cisco Unified Border Element (Cisco UBE). This feature adds Simple Network Management Protocol (SNMP) support for displaying Cisco UBE status (show cube status) by implementing the CISCO-UBE-MIB. The mode border-element command is enhanced to set the license capacity of Cisco UBE and enable the display of Cisco UBE status using the show cube status command.
Cisco UBE Support for Domain-Based Routing

For detailed information about this feature, see the following document:


Cisco UBE Support for SRTP-RTP Internetworking

For detailed information about this feature, see the following document:


Cisco UBE VQM

Video Quality Monitoring (VQM) enables you to monitor and compare video quality between two networks. VQM on the Cisco Unified Border Element (Cisco UBE) monitors Cisco UBE video flows in a non-intrusive manner and presents the video quality as a mean opinion score (MOS).

For more information, see the following document:


Cisco Unified CME/SRST 8.8

For detailed information about this feature, see the following documents:


Configuring Support for Dynamic REFER Handling on the Cisco UBE

For detailed information about this feature, see the following document:


DHCP—Automatic IPv4 Address Pool Assignment for DMVPN Spokes

For detailed information about this feature, see the following document:


EIGRP/SAF HMAC-SHA-256 Authentication

For detailed information about this feature, see the following document:

Enhanced NBAR

For detailed information about this feature, see the following document:

GDOI MIB Support for GET VPN

For detailed information about this feature, see the following document:

GET VPN GM Removal and Policy Trigger

For detailed information about this feature, see the following document:

IKEv2 Headend Support for Remote Access Clients—Anyconnect, Win7 IPv6, Flexvpn Hardware Client

For detailed information about this feature, see the following document:

IKEv2 Remote Access Hardware Client

For detailed information about this feature, see the following document:

IPv6 Transport for DMVPN

For detailed information about this feature, see the following document:

Legacy QoS Command Deprecation: Removed Commands

For detailed information about this feature, see the following document:

Medianet Metadata

For detailed information about this feature, see the following document:
**MGF OIR Support for Service Modules**

For detailed information about this feature, see the following document:


**mGRE Tunnel Support over IPv6**

For detailed information about this feature, see the following documents:


**MPLS TE over GRE Tunnel Support**

For detailed information about this feature, see the following documents:


**Multicast Music-on-Hold Support on the Cisco UBE**

For detailed information about this feature, see the following document:


**Multi-SA for DVTI**

For detailed information about this feature, see the following document:


**Network-Based Recording Using the Cisco UBE**

For detailed information about this feature, see the following document:


**OSPFv3 Address Families**

For detailed information about this feature, see the following documents:


**OSPFv3 Manet Extensions**

For detailed information about this feature, see the following document:

New and Changed Information

**Overhead Accounting**

For detailed information about this feature, see the following document:


**PfR RSVP Control**

For detailed information about this feature, see the following document:


**PfR/RSVP CAC Integration**

For detailed information about this feature, see the following document:


**Public Key Infrastructure IPv6 Support for VPN Solutions**

Encryption and IPv6 support for the following commands was added:

- The `crypto pki export pem` command was modified. Support was added in the CLI for hiding the password in an exported PEM-formatted file with the introduction of the `password` keyword followed by the `passwordphrase` argument.

- The `crypto pki export pkcs12` password was modified. Support was added in the CLI for hiding the password in an exported PKCS12-formatted file with the introduction of the `password` keyword followed by the `passwordphrase` argument.

- The `crypto pki import pem` command was modified. Support was added in the CLI for hiding the password in an imported PEM-formatted file with the introduction of the `password` keyword followed by the `passwordphrase` argument.

- The `crypto pki import pkcs12 password` command was modified. Support was added in the CLI for hiding the password in an imported PKCS12-formatted file with the introduction of the `password` keyword followed by the `passwordphrase` argument.

- The `enrollment url (ca-trustpoint)` command was modified. Support for specifying the IPv6 address in a URL for the CA was added.

- The `ip-address (ca-trustpoint)` command was modified. Support for specifying the IPv6 address in the certificate request was added.

- The `ocsp url` command was modified. Support for specifying the IPv6 address in a URL for the OCSP server was added.

For detailed information about this feature, see the following documents:


RADIUS over IPv6

For detailed information about this feature, see the following document:

Right to Use (RTU) Licensing Support in CLIs and MIBs for ISR G2 Platforms

For detailed information about this feature, see the following document:

SAF Dynamic Neighbors

For detailed information about this feature, see the following document:

Seamless Rate Adaptation on VDSL2/ADSL Multimode SKUs

For detailed information about this feature, see the following documents:

SRE Installation and Image Management Enhancements

For detailed information about this feature, see the following document:

T.38 Fax Support on the Cisco UBE for IPv6

For detailed information about this feature, see the following document:
TACACS over IPv6

For detailed information about this feature, see the following document:


Temperature and Voltage Monitoring

The Cisco Connected Grid Router 2010 includes sensors that measure the status and internal temperature of critical components. Internal component temperatures are measured for the central processor, internal components, and interface cards. By default, a 72-hour temperature history is stored for the central processor at one-hour intervals.

Power consumption and power supplies are monitored. The measured temperature is compared to predetermined threshold limits and, if the temperature does not fall within the limits, the information is recorded and a warning sent to the system administrator by means of Simple Network Management Protocol (SNMP) traps until the temperature falls back to its normal range.

You can store historical temperature and power supply voltage data. New `show` commands have been added to allow you to check the temperature and power supply voltage history configuration and data. For additional details, see the Cisco Connected Grid Router 2010 Software Configuration Guide at the following URL:


TFTP—Blocksize Option

For detailed information about this feature, see the following document:


UBR+ on VDSL2/ADSL Multimode SKUs

UBR+ is a special ATM service class developed by Cisco Systems. While UBR defines only peak cell rate (PCR), UBR+ also defines an MCR and (on the switch) a cell delay variation tolerance (CDVT).

Cisco IOS Release 15.2(1)T adds support for UBR+ on the Cisco 886VA, 887VA, and 887VA-M.

VMI QoS

For detailed information about this feature, see the following document:


Important Notes

The following information applies to all releases of Cisco IOS Release 15.2T.

- Cisco IOS Behavior Changes, page 73
- Field Notices and Software-Related Tools and Information, page 76
Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in this section.

Behavior changes are provided for the following releases:

- Cisco IOS Release 15.2(1)T4, page 73
- Cisco IOS Release 15.2(1)T3, page 73
- Cisco IOS Release 15.2(1)T2, page 74
- Cisco IOS Release 15.2(1)T1, page 75

Cisco IOS Release 15.2(1)T4

The following behavior changes are introduced in Cisco IOS Release 15.2(1)T4:

- BGP Processing of the Removal of Private AS Numbers from AS Path.

  Old Behavior: When the `neighbor remove-private-as` command is configured and a route-map without a continue clause is configured, the processing order is:
  
  1. `neighbor remove-private-as` processing
  2. `set as-path prepend` or `set as-path prepend last-as`

  However, if the route-map contains a continue clause, the processing order is reversed.

  New Behavior: When the `neighbor remove-private-as` command is configured and a route-map is configured (whether it has a continue clause or not), the processing order is always:

  1. `neighbor remove-private-as` processing
  2. `set as-path prepend` or `set as-path prepend last-as`

- Initial INVITE with 0.0.0.0 call flow is supported.

  Old Behavior: Initial INVITE with 0.0.0.0 is not supported unless ACK contains valid ip address.

  New Behavior: This call flow is supported.

  Additional Information:


- IPv6 support is added for legacy Control Plane Policing (CoPP) on Cisco Express forwarding interfaces.

  Old Behavior: IPv6 support is not available for CoPP, resulting in a failure of policing and rate limiting.

  New Behavior: IPv6 support is added for legacy CoPP on Cisco Express forwarding interfaces that support aggregate-scope policing and rate limiting.

Cisco IOS Release 15.2(1)T3

The following behavior changes are introduced in Cisco IOS Release 15.2(1)T3:
- PfR syslog levels have been added to minimize the number of messages.
  Old Behavior: Too many PfR syslog messages are generated.
  New Behavior: PfR syslog levels have been added to minimize the number of messages displayed, and a syslog notice has been added to display when 30 percent of the traffic classes are out-of-policy.

- Fast Network Time Protocol (NTP) synchronization is achieved.
  Old Behavior: The burst and initial burst (iburst) modes are enabled manually.
  New Behavior: The burst and iburst modes are enabled by default.

- The telecom-solutions keyword is not supported.
  Old Behavior: The telecom-solutions keyword in the ntp refclock command allows users to configure the reference clock driver.
  New Behavior: Effective with CSCtu20233, the telecom-solutions keyword, along with its options, is visible but cannot be configured.

Cisco IOS Release 15.2(1)T2

The following behavior changes are introduced in Cisco IOS Release 15.2(1)T2:

- Output from the show policy-map command does not display the default burst rate; however, the output does display the user-specified burst rate.
  Old Behavior: Output from the show policy-map command displays the default burst rate.
  New Behavior: Output from the show policy-map command does not display the default burst rate. The output does display the burst rate specified by the police command in a policy map.

- BGP scan time range is changed.
  Old Behavior: The bgp scan-time command has a scanner-interval range of 15-60 seconds. The bgp scan-time command cannot be configured (it remains at the default value of 60 seconds) if BGP Next Hop Tracking (NHT) is configured (by the bgp nexthop command).
  New Behavior: The bgp scan-time command has a scanner-interval range of 5-60 seconds. The bgp scan-time command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the bgp nexthop command).

- CSCtu80224
  BGP next-hop for redistributed recursive static routes is changed.
Old Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next hop to be itself. The local next-hop (equal to next-hop-self) is kept.
New Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be the recursive next-hop of the static route.

- Maximum number of traffic classes (prefixes) to be learned in a PfR learn list is increased.
  Old Behavior: Using the Cisco IOS CLI, count (PfR) command, the maximum number of traffic classes to be learned in a PfR learn list was 100, with a default of 50.
  New Behavior: Using the Cisco IOS CLI, count (PfR) command, the maximum number of traffic classes to be learned in a PfR learn list is 1000, with a default of 1000.

- Server and user-agent SIP headers now have only token characters.
  Old Behavior: Outgoing SIP messages have nontoken characters in server and user-agent SIP headers.
  New Behavior: Server and user-agent SIP headers have only token characters.

- New keywords standard and system are added to existing dtmf-interworking CLI under voice service and dial-peer configuration modes.
  Old Behavior: SIP INFO dtmf digit to RFC4733 DTMF interworking was not supported.
  New Behavior: The newly added keyword standard generates RTP NTE packets that are RFC 4733 compliant.

- Analogue vm-integration is added to SIP line.
  Old behavior: vm-integration only applies to SCCP line.
  New behavior: vm-integration also applies to SIP line.
  Additional Information:
  1. The chapter was updated to apply both to SCCP and SIP.
  2. Added call-forward b2bua busy and call-forward b2bua noan commands to configure vm-integration for SIP line.

**Cisco IOS Release 15.2(1)T1**

The following behavior changes are introduced in Cisco IOS Release 15.2(1)T1:
• Increase in autonomous system number or community prepending in BGP Inbound Optimization using PfR.

    Old Behavior: In both the “BGP Autonomous System Number Prepend” and “BGP Autonomous System Number Community Prepend” methods of controlling inside prefixes using PfR, the number is increased one by one up to the maximum of six ASes in unreachable, loss, and delay OOP cases.

    New Behavior: In both the “BGP Autonomous System Number Prepend” and “BGP Autonomous System Number Community Prepend” methods of controlling inside prefixes using PfR, the new behavior increases the AS number or community to the maximum of six immediately, or it decreases to zero in unreachable and loss OOP cases.

    In the delay OOP case, the behavior is the same as the old behavior.


• Documentation changes to support the hiding of the Optimized Edge Routing (OER) CLI.

    Old Behavior: OER border router functionality is supported on the Catalyst 6500 switch.

    New Behavior: OER is no longer supported on the Catalyst 6500 switch, and the OER CLI is hidden.


• Multiple Crypto Engines.

    Old Behavior: When a powerful crypto engine starts, it disables the less powerful crypto engine and handles all IPv4 and IPv6 crypto functions.

    New Behavior: If there are multiple crypto engines in a network that has IPv4 and IPv6 traffic, one crypto engine handles IPv4 traffic and another crypto engine handles IPv6 traffic. It is also possible that one crypto engine handles both IPv4 and IPv6 traffic.


Field Notices and Software-Related Tools and Information

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at http://www.cisco.com/cisco/web/download/index.html.
Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug.

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note

If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

This document contains the following sections:

- Using the Cisco Bug Search Tool, page 78
- Resolved Bugs—Cisco IOS Release 15.2(4)M11, page 79
- Resolved Bugs—Cisco IOS Release 15.2(4)M10, page 79
- Resolved Bugs—Cisco IOS Release 15.2(4)M9, page 80
- Resolved Bugs—Cisco IOS Release 15.2(4)M8, page 81
- Resolved Bugs—Cisco IOS Release 15.2(4)M7, page 82
- Resolved Bugs—Cisco IOS Release 15.2(4)M6a, page 82
- Resolved Bugs—Cisco IOS Release 15.2(4)M6, page 83
- Resolved Bugs—Cisco IOS Release 15.2(4)M5, page 86
- Resolved Bugs—Cisco IOS Release 15.2(4)M4, page 88
Using the Cisco Bug Search Tool

The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested. In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

For more information about how to use the Cisco Bug Search Tool, including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ.

Note
You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

To use the Cisco Bug Search Tool:

1. In your browser, navigate to the Cisco Bug Search Tool.
2. If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.
3. To search for a specific bug, enter the bug ID in the Search For field and press Enter.
4. To search for bugs related to a specific software release, do the following:
   a. In the Product field, choose Series/Model from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.
   b. In the Releases field, enter the release for which you want to see bugs.

The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria. You can mouse over bugs to see more content about a specific bug.

5. To see more content about a specific bug, you can do the following:
   - Mouse over a bug in the preview to display a pop-up with more information about that bug.
   - Click on the hyperlinked bug headline to open a page with the detailed bug information.
To restrict the results of a search, choose from one or more of the following filters:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modified Date</td>
<td>A predefined date range, such as last week or last six months.</td>
</tr>
<tr>
<td>Status</td>
<td>A specific type of bug, such as open or fixed.</td>
</tr>
<tr>
<td>Severity</td>
<td>The bug severity level as defined by Cisco. For definitions of the bug severity levels, see Bug Search Tool Help &amp; FAQ.</td>
</tr>
<tr>
<td>Rating</td>
<td>The rating assigned to the bug by users of the Cisco Bug Search Tool.</td>
</tr>
<tr>
<td>Support Cases</td>
<td>Whether a support case has been opened or not.</td>
</tr>
</tbody>
</table>

Your search results update when you choose a filter.

## Resolved Bugs—Cisco IOS Release 15.2(4)M11

### Table 1  Resolved Bugs—Cisco IOS Release 15.2(4)M11

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCup90532</td>
<td>Cisco IOS and IOS XE Software DNS Forwarder Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCuz81292</td>
<td>IPv6 neighbor discovery packet processing behavior</td>
</tr>
<tr>
<td>CSCuz25390</td>
<td>IP tunnel inconsistencies cause memory corruption, crash</td>
</tr>
<tr>
<td>CSCux97540</td>
<td>Cisco IOS and IOS-XE IKEv2 DoS Vulnerability</td>
</tr>
<tr>
<td>CSCvb29204</td>
<td>Benign Certain on IOS and IOS-XE</td>
</tr>
<tr>
<td>CSCuy47382</td>
<td>Cisco IOS and IOS XE Software IKEv1 1 Fragmentation Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCuy87667</td>
<td>Cisco IOS and IOS XE Software AAA Login Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvb16274</td>
<td>PPTP Start-Control-Connection-Reply packet leaks router memory contents</td>
</tr>
</tbody>
</table>

## Resolved Bugs—Cisco IOS Release 15.2(4)M10

### Table 2  Resolved Bugs—Cisco IOS Release 15.2(4)M10

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCut42645</td>
<td>input queue wedged on a SSLVPN enabled router</td>
</tr>
<tr>
<td>CScux38417</td>
<td>IOS and IOS-XE IKEv2 Fragmentation DoS</td>
</tr>
<tr>
<td>CSCuo82943</td>
<td>DMVPN: Leak observed in SADB Peering Chunk</td>
</tr>
<tr>
<td>CSCum32910</td>
<td>Memory Leak due to SADB Peering Ch</td>
</tr>
<tr>
<td>CSCur18715</td>
<td>CUCM native queue call disconnect due to Application AckTimer expire</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCuq59708</td>
<td>SSTE: Crash seen at l4f_set_tcp_option on passing malformed packets</td>
</tr>
<tr>
<td>CSCuw85826</td>
<td>Evaluation of Cisco IOS and IOS-XE for NTP_October_2015</td>
</tr>
<tr>
<td>CSCul01067</td>
<td>Memory leak in NTP client with IPv6 configuration</td>
</tr>
<tr>
<td>CSCum65703</td>
<td>Inconsistency on config &quot;privileged&quot; commands as seen in running-config</td>
</tr>
<tr>
<td>CSCUs75471</td>
<td>MALLOCFAIL on &quot;Shell Pipeline Process&quot; When Issuing &quot;Show log</td>
</tr>
<tr>
<td>CSCus23013</td>
<td>show cmd under &quot;parser view include-exclude&quot; cause standby router to reload</td>
</tr>
</tbody>
</table>

**Resolved Bugs—Cisco IOS Release 15.2(4)M9**

**Table 3**  
Resolved Bugs—Cisco IOS Release 15.2(4)M9

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuu18788</td>
<td>DATACORRUPTION-1-DATAINCONSISTENCY when polling ceExtSysBootImageList</td>
</tr>
<tr>
<td>CSCum73170</td>
<td>Unable to collect sufficient entropy</td>
</tr>
<tr>
<td>CSCus52216</td>
<td>IOS MGCP GW payload type changes from 101 to 118 on xfer call for V.150</td>
</tr>
<tr>
<td>CSCuq36627</td>
<td>WAAS Express: Failed to create SSL session. (no available resources)</td>
</tr>
<tr>
<td>CSCuo70451</td>
<td>IPS: Crash@ips_dp_delete_half_open_session seen after heavy HTTP traffic</td>
</tr>
<tr>
<td>CSCuu00059</td>
<td>IOS ZBFW Not Clearing Half-open MSRPC sessions</td>
</tr>
<tr>
<td>CSCur63914</td>
<td>IOS ZBFW Not Clearing Half-open MSRPC sessions &amp; MSRPC session hang</td>
</tr>
<tr>
<td>CSCur29582</td>
<td>IPSEC-VPN: removal of &quot;crypto-map&quot; kills BFD session forever</td>
</tr>
<tr>
<td>CSCur71700</td>
<td>Fine tuning of Tx interrupt coalescing in c3900 when tx-ring 4</td>
</tr>
<tr>
<td>CSCuh36583</td>
<td>ISRG2 - DSP Crash due to Backplane Switch Lockup During T1 Errors</td>
</tr>
<tr>
<td>CSCut40341</td>
<td>Line protocol on SM-X-1T3/E3 configured for frame-relay remains down</td>
</tr>
<tr>
<td>CSCur07571</td>
<td>Processor memory leak with MRCP_Client at cc_api_get_call_active_entry</td>
</tr>
<tr>
<td>CSCut77619</td>
<td>APRIL 2015 NTPd Vulnerabilities</td>
</tr>
<tr>
<td>CSCun71393</td>
<td>crash when polling the cntpPeersVarEntry MIB</td>
</tr>
<tr>
<td>CSCul73513</td>
<td>Server-client clock not in sync after leap configuration</td>
</tr>
<tr>
<td>CSCut63500</td>
<td>dot1q encapsulation causes vam2+ to crash</td>
</tr>
<tr>
<td>CSCUs77875</td>
<td>List Headers leak verified cert chain Held CCSIP_TLS_SOCKET &amp; Chunk Mgr</td>
</tr>
<tr>
<td>CSCtn75051</td>
<td>%SYS-3-TIMERNEG: Cannot start timer with negative offset</td>
</tr>
<tr>
<td>CSCuu82607</td>
<td>Evaluation of all for OpenSSL June 2015</td>
</tr>
<tr>
<td>CSCuq74492</td>
<td>IOS/IOSd Multiple Vulnerabilities in OpenSSL - August 2014</td>
</tr>
<tr>
<td>CSCus61884</td>
<td>JANUARY 2015 OpenSSL Vulnerabilities</td>
</tr>
<tr>
<td>CSCut46130</td>
<td>MARCH 2015 OpenSSL Vulnerabilities</td>
</tr>
<tr>
<td>CSCun86268</td>
<td>sslvpn: route not installed in routing table of vrf - received from AAA</td>
</tr>
</tbody>
</table>
## Resolved Bugs—Cisco IOS Release 15.2(4)M8

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCts39290</td>
<td>Underruns incrementing for native interfaces of NPE-G1.</td>
</tr>
<tr>
<td>CSCua01375</td>
<td>LDAP VRF is not working with PKI.</td>
</tr>
<tr>
<td>CSCub45809</td>
<td>Providing a CLI knob for handling media loops in VoIP RTP.</td>
</tr>
<tr>
<td>CSCuc98021</td>
<td>One way audio over Cisco UBE after session refresh.</td>
</tr>
<tr>
<td>CSCud35669</td>
<td>Cisco IOS Release 15.5(3)M ISM-Reventon: IPv6 EIGRP routing does not work over DVTI with reventon.</td>
</tr>
<tr>
<td>CSCuh49066</td>
<td>Standby crashes due to LBL sync on “parser view li-view”.</td>
</tr>
<tr>
<td>CSCuh56446</td>
<td>Webauth: “Framed-IP-Address” in the accounting START and STOP requests.</td>
</tr>
<tr>
<td>CSCui08221</td>
<td>A voice gateway reloaded unexpectedly due to a bus error.</td>
</tr>
<tr>
<td>CSCuij17818</td>
<td>PPPOE_DISCOVERY packets stuck in input_queue after PADT has been sent.</td>
</tr>
<tr>
<td>CSCui49375</td>
<td>Cisco ASR 1000 Series Routers: %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0).</td>
</tr>
<tr>
<td>CSCui52326</td>
<td>L2TP/Ipsec with NAT-T to ISR-G2 with ISM-VPN module fails.</td>
</tr>
<tr>
<td>CSCui70788</td>
<td>Router crashes when calculating the best cost successor in EIGRP DUAL.</td>
</tr>
<tr>
<td>CSCum36951</td>
<td>Cisco IOS Software IKEv2 denial-of-service vulnerabilities.</td>
</tr>
<tr>
<td>CSCum48166</td>
<td>Cisco c2821/124-24.T8/ router 2811 crash due to Process= DSMP.</td>
</tr>
<tr>
<td>CSCum94811</td>
<td>TCP packet memory leak vulnerability.</td>
</tr>
<tr>
<td>CSCum96955</td>
<td>SSST: Router crash @ ether_extract_addr, mace_dp_feature_action_pre_waas.</td>
</tr>
<tr>
<td>CSCun62014</td>
<td>Router crash with %SYS-3-BADFREETRAS after reconfiguring PPPOE.</td>
</tr>
<tr>
<td>CSCuo55180</td>
<td>Cisco ASR 1000 Series Routers with PPPOE subscribers block overrun crash.</td>
</tr>
<tr>
<td>CSCuo75572</td>
<td>Cisco IOS Software IKEv2 denial-of-service vulnerabilities.</td>
</tr>
<tr>
<td>CSCuo95771</td>
<td>IPsec SA are deleted incorrectly by background process.</td>
</tr>
<tr>
<td>CSCup26595</td>
<td>The address and control fields of the PPP header are removed unexpectedly.</td>
</tr>
<tr>
<td>CSCup43333</td>
<td>Crash due to avl_search.</td>
</tr>
<tr>
<td>CSCup58405</td>
<td>Router crash at __be_sipAppProbeHeaderPresence.</td>
</tr>
<tr>
<td>CSCup67654</td>
<td>ISM-VPN module crashes due to memory leak, -Traceback= 1000b8a0.</td>
</tr>
<tr>
<td>CSCuq5240</td>
<td>Cisco UBE consumes reinvite when m=audio line has more than 1 codec.</td>
</tr>
<tr>
<td>CSCuq36941</td>
<td>Issue with MRCPv2 tcpip with VXML 3945e gateway.</td>
</tr>
<tr>
<td>CSCuq43266</td>
<td>VXML gateway Crash @msw_reco_start process.</td>
</tr>
<tr>
<td>CSCuq74774</td>
<td>Cisco UBE not opening random UDP ports for SIP.</td>
</tr>
<tr>
<td>CSCuq66242</td>
<td>Zone-based firewall+ ISM+ DMVPN requires explicit permit for GRE traffic.</td>
</tr>
<tr>
<td>CSCuq93406</td>
<td>IOSd crash on Ethernet CFM receiving a malformed CFM frame.</td>
</tr>
<tr>
<td>CSCuq99173</td>
<td>Conditions experienced parsing H.225 packet may cause crash.</td>
</tr>
<tr>
<td>CSCu07269</td>
<td>QoS is causing alignment errors on MLPPP E1 interfaces.</td>
</tr>
<tr>
<td>CSCu13495</td>
<td>Service data of a service change is not updated by SAF forwarder.</td>
</tr>
<tr>
<td>CSCu16675</td>
<td>VXML gateway Crash @ms_handle_stream_timer.</td>
</tr>
<tr>
<td>CSCu21757</td>
<td>Memory leak <em>Dead</em> = AFW_application_process and QSIG-rose.</td>
</tr>
<tr>
<td>CSCu23656</td>
<td>Cisco IOS and IOSd in Cisco IOS XE Release: Evaluation of SSLv3 POODLE vulnerability.</td>
</tr>
<tr>
<td>CSCu25315</td>
<td>Router crash: QoS group of packet is greater than 1023.</td>
</tr>
</tbody>
</table>
Open and Resolved Bugs

Resolved Bugs—Cisco IOS Release 15.2(4)M7

All resolved bugs for this release are available in the Cisco Bug Search Tool through the fixed bug search.

This search uses the following search criteria and filters:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Series/Model Cisco IOS and NX-OS Software =&gt; Cisco IOS</td>
</tr>
<tr>
<td>Release</td>
<td>15.2(4)M7</td>
</tr>
<tr>
<td>Status</td>
<td>Fixed</td>
</tr>
<tr>
<td>Severity</td>
<td>2 or higher</td>
</tr>
</tbody>
</table>

Resolved Bugs—Cisco IOS Release 15.2(4)M6a

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCue23898</td>
<td>IOS bus error crash when saving the running configuration</td>
</tr>
<tr>
<td>CSCuc55402</td>
<td>ISM- SA comes up but data forwarding fails</td>
</tr>
<tr>
<td>CSCui55556</td>
<td>ISR CUBE crashes at function local_xcode_rtp_xmit</td>
</tr>
<tr>
<td>CSCum90509</td>
<td>No RTP Connections for RSVP Features in XE3.7 image</td>
</tr>
<tr>
<td>CSCud86991</td>
<td>ASR1K iosd crash with &quot;crypto dynamic-map&quot; config</td>
</tr>
<tr>
<td>CSCum93484</td>
<td>Mem leak due to CryptoIKMP while allocating memory for AAA attribute list</td>
</tr>
</tbody>
</table>

CSCur33686 ISM fails to delete active IPsec-Session SPI leakage.
CSCur40808 ISM-VPN: QoS preclassify not preserving the QoS markings.
CSCur62223 Router stops all traffic out of MFR link with crypto map with ISM module.
CSCur79561 A router crashed due to a divide by zero.
CSCur83129 Error message: SOC4E COMMAND FAIL seen in live network.
CSCur85454 VXML GW fails to handoff call to VXML application.
CSCur87077 Ping failure is seen when annexe F & G is configured.
CSCur99303 Calls are disconnected after receiving A3-B7.
CSCus48378 CNS feature required to support TLS.
CSCus48386 LDAPv3 client REQUIRED to support TLS.
CSCus48493 IOS SSLVPN required to support TLS.
CSCus75537 Add the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite support for VXML HTTPC.
CSCut55517 Memory corruption due to crypto PKI.
<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuj19201</td>
<td>TBAR Refresh Causes Re-registration Time Re-calculation on GMs</td>
</tr>
<tr>
<td>CSCui85371</td>
<td>ASR1K:ikev2_ecdsa: Ikev2 session is NOT coming UP</td>
</tr>
<tr>
<td>CSCul27924</td>
<td>IOSd crash at crypto_ike_find_profile while strcmp</td>
</tr>
<tr>
<td>CSCum83923</td>
<td>Input Error Counter Mismatch on Serial Interface</td>
</tr>
<tr>
<td>CSCul04503</td>
<td>ATM PVC stays down though the SHDSL controller is up</td>
</tr>
<tr>
<td>CSCui83823</td>
<td>SSHV2 session closes prematurely via telnet and putty</td>
</tr>
<tr>
<td>CSCun91252</td>
<td>3925e crashing when sip-ua point to DNS and is removed</td>
</tr>
<tr>
<td>CSCui19224</td>
<td>Modem gone bad with locked SIM after reload</td>
</tr>
</tbody>
</table>

### Resolved Bugs—Cisco IOS Release 15.2(4)M6

#### Table 6

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCs80209</td>
<td>IOS running device may crash adding or removing &quot;login block-for&quot;</td>
</tr>
<tr>
<td>CSCuh72031</td>
<td>Nile SE4: Crash seen at tacacs_plus_get_nat_addr with send-nat-address</td>
</tr>
<tr>
<td>CSCue95644</td>
<td>Remove type 4 hashing</td>
</tr>
<tr>
<td>CSCtx20903</td>
<td>TACACS authenproblem between CISCO switch - errno 257((ENOTCONN))</td>
</tr>
<tr>
<td>CSCuz73473</td>
<td>%IPRT-3-INVALID_NEXTHOP upon importing multipath with maxi paths in vrf</td>
</tr>
<tr>
<td>CSCu899819</td>
<td>LSM and MVPN traffic dropping after clear BGP * with TE Tunnel</td>
</tr>
<tr>
<td>CSCue68714</td>
<td>OVLD: BFD BGP Client Incompatibility between IOS t-train and IOSXE</td>
</tr>
<tr>
<td>CSCul96778</td>
<td>Router crash at bgp_topo_valid_tid</td>
</tr>
<tr>
<td>CSCuc60868</td>
<td>Router Crash on uncfg &amp; reconfig of VPLS BGP Signaling - Script Run</td>
</tr>
<tr>
<td>CSCui65083</td>
<td>COS match not preserved on dot1Q interface with reload</td>
</tr>
<tr>
<td>CSCug15952</td>
<td>Sbty RP crash: %QOS-3-INDEX_EXISTS, HA bulk sync and self Reload</td>
</tr>
<tr>
<td>CSCui10167</td>
<td>7201 15.2(4)M4 -- ZBF resets TCP conn with &quot;ip tcp adjust-mss&quot;</td>
</tr>
<tr>
<td>CSCui42069</td>
<td>Wrong QoS classification with nested classes.</td>
</tr>
<tr>
<td>CSCbu45763</td>
<td>crash following SYS-2-FREEFREE and SYS-6-MTRACE messages</td>
</tr>
<tr>
<td>CSCui03965</td>
<td>ISSU XE392-&gt;XE310 Config-sync@commands configure include interface</td>
</tr>
<tr>
<td>CSCuh05259</td>
<td>file prompt quiet cli dont work with config replace cli</td>
</tr>
<tr>
<td>CSCuh53075</td>
<td>C3900's ISM crashed when &quot;clear crypto session&quot; with 3k DMVPN tunnels</td>
</tr>
<tr>
<td>CSCul00904</td>
<td>c3900's ISM module crashed with DMVPN</td>
</tr>
<tr>
<td>CSCuj95960</td>
<td>ISM Crash due to reassembly Double free</td>
</tr>
<tr>
<td>CSCuj77430</td>
<td>ISM-VPN drops deny crypto acl traffic instead of passing it in clear</td>
</tr>
<tr>
<td>CSCuh15473</td>
<td>Pi22: Spurious memory access made and ISM-VPN crashes with low mtu value</td>
</tr>
<tr>
<td>CSCud72245</td>
<td>Traceback found at reventon_handler_ib_passthrough</td>
</tr>
<tr>
<td>CSCuj29428</td>
<td>%SYS-SW1-2-INTSCHED: 'sleep for' at level 2 -Process= &quot;Init&quot;</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCui84344</td>
<td>Outbound IPSec Sequence No. not synced from Active to Standby 3900E</td>
</tr>
<tr>
<td>CSCu66558</td>
<td>security license mandatory for 3G HWIC /LTE HWIC with dialer-watch</td>
</tr>
<tr>
<td>CSCul41475</td>
<td>TCP DNS request may cause a memory leak</td>
</tr>
<tr>
<td>CSCug19522</td>
<td>Device gets Trusted IP while dot1x performed in the background</td>
</tr>
<tr>
<td>CSCui55899</td>
<td>Negotiation not happening between authenticator and supplicant</td>
</tr>
<tr>
<td>CSCuh27343</td>
<td>Cube crashed while Running UCCX Outbound Load with CPA enabled</td>
</tr>
<tr>
<td>CSCug37304</td>
<td>Router running IOS may crash - Seen in SCCP controlled FXS config</td>
</tr>
<tr>
<td>CSCua63182</td>
<td>EIGRP min BW is calculated incorrectly for ngbrs of varying versions</td>
</tr>
<tr>
<td>CSCuc99750</td>
<td>EIGRP routes which are not FS making it to the routing table</td>
</tr>
<tr>
<td>CSCuj30572</td>
<td>Router crash @ eigrp_pfr_get_drdb with PFR and OER</td>
</tr>
<tr>
<td>CSCuh56385</td>
<td>SAF:ISR: Service Routing delays in data exchange on peer forwarders</td>
</tr>
<tr>
<td>CSCuh94035</td>
<td>Watchdog crash while EIGRP updates Topology Table</td>
</tr>
<tr>
<td>CSCuj05643</td>
<td>FNF alignment errors lead to high CPU</td>
</tr>
<tr>
<td>CSCui42172</td>
<td>&quot;cufwConnGlobalNumHalfOpen&quot; MIB not reporting correctly</td>
</tr>
<tr>
<td>CSCui15047</td>
<td>Crash at fw_dp_insp_appl_handle_close_control_stream</td>
</tr>
<tr>
<td>CSCua49735</td>
<td>WExp Router got crashed while running stress test</td>
</tr>
<tr>
<td>CSCuh72000</td>
<td>PI doesn't copy TOS from mpls header to IP/GRE header</td>
</tr>
<tr>
<td>CSCuj27671</td>
<td>QUAD SUP2T VSS Failover fails with tunnel path-mtu-discovery config</td>
</tr>
<tr>
<td>CSCui87667</td>
<td>The copy from MPLS exp bits to IP tos is done without the left shift</td>
</tr>
<tr>
<td>CSCuj39400</td>
<td>Bus Error Crash @ __be_voip_remote_rtcp_packet</td>
</tr>
<tr>
<td>CSCui26458</td>
<td>Calls with multiple M-lines on SDP can hung UDP ports on CUBE</td>
</tr>
<tr>
<td>CSCud62864</td>
<td>CUBE consuming sendrcv reinvite when midcall reinvite consumption active</td>
</tr>
<tr>
<td>CSCuj58299</td>
<td>CUBE Input queue wedge RTCP packets - 180w/o SDP followed by 180w/SDP</td>
</tr>
<tr>
<td>CSCuh68961</td>
<td>CUBE is failing to pass reInvite in DO-DO scenario</td>
</tr>
<tr>
<td>CSCtz97777</td>
<td>ipipgw crash SYS-2-FREEFREE at ccsip_update_srtp_caps</td>
</tr>
<tr>
<td>CSCui96893</td>
<td>Router hangs at avl_search and crypto_ipsec_get_any_sa_with_flowid</td>
</tr>
<tr>
<td>CSCug14423</td>
<td>A packet gets dropped when bring UP spoke-spoke session in DmVPN</td>
</tr>
<tr>
<td>CSCuj47795</td>
<td>Anti-replay protection disabled when using IKEv2 and AES-GMC or AES-GMAC</td>
</tr>
<tr>
<td>SCCum61595</td>
<td>ALIGN-3-TRACE @ ikmp_enqueue_cert_request</td>
</tr>
<tr>
<td>CSCum22612</td>
<td>ASR1k IKE SA Stuck in MM_KEY_EXCH with RSA-SIG blocking new SAs with CAC</td>
</tr>
<tr>
<td>CSCui13619</td>
<td>ipv6 esp packet is recirculated and dropped after decryption</td>
</tr>
<tr>
<td>CSCui82817</td>
<td>Advertisement of TE-Tunnels with absolute metric is inconsistent</td>
</tr>
<tr>
<td>CSCtn96442</td>
<td>%ALIGN-3-TRACE dlsar_post_coalesce_rx</td>
</tr>
<tr>
<td>CSCui63171</td>
<td>IOS crash when IP CEF is enabled &amp; clearing out NAT translations</td>
</tr>
<tr>
<td>CSCui53593</td>
<td>ACL filter for QOS classification does not work when CEF is enabled.</td>
</tr>
<tr>
<td>CSCui03432</td>
<td>3900e goes Unresponsive and output queue gets full - interfaces wedged</td>
</tr>
<tr>
<td>CSCuj32782</td>
<td>cmCallerID in CISCO-MODEM-MGMT-MIB has issues when there is no caller-id</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCun35849</td>
<td>KeepAlive to check status of NPU and to reload if NPU is not responding</td>
</tr>
<tr>
<td>CSCuh80914</td>
<td>PPP Multilink Fragment Size - Packet drops with HWIC-4SHDSL</td>
</tr>
<tr>
<td>CSCuh12639</td>
<td>3900 service module interface always in promiscuous mode</td>
</tr>
<tr>
<td>CSCuh69292</td>
<td>LDAP gets in stuck state even if PKI provides finite timeout</td>
</tr>
<tr>
<td>CSCuh41290</td>
<td>PKI with LDAP gets in stuck state due to infinite LDAP timer</td>
</tr>
<tr>
<td>CSCuj62593</td>
<td>MALLOCFAIL during mrcp calls load</td>
</tr>
<tr>
<td>CSCuj20120</td>
<td>NAT-PT router fails to create a NAT table</td>
</tr>
<tr>
<td>CSCui01168</td>
<td>PI19:NBAR punts packets causing high CPU</td>
</tr>
<tr>
<td>CSCui59004</td>
<td>iosd crash while configuring no ntp server</td>
</tr>
<tr>
<td>CSCuj11576</td>
<td>7200VXR stack corruption crash: BFD process</td>
</tr>
<tr>
<td>CSCug99771</td>
<td>OSPF N2 default route missing from Spoke upon reloadin g Hub</td>
</tr>
<tr>
<td>CSCui21030</td>
<td>OSPFv2 RI LSA from third party vendor causes memory corruption</td>
</tr>
<tr>
<td>CSCui54254</td>
<td>OSPFv3 may not flush some apparently self-originated LSAs</td>
</tr>
<tr>
<td>CSCuj50371</td>
<td>VSA : Encryption Failure with IPsec HA and SSO</td>
</tr>
<tr>
<td>CSCum94408</td>
<td>IOS PKI Public Key caching fails during IKE MM6 Signature verification</td>
</tr>
<tr>
<td>CSCui07002</td>
<td>PKI chain-validation seg fault process Crypto PKI-CRL if CRL is expired</td>
</tr>
<tr>
<td>CSCui82843</td>
<td>Qos markings not preserved when crypto map is applied</td>
</tr>
<tr>
<td>CSCuh36124</td>
<td>SAF:ISR: Service Routing HIGH cpu on failover condition</td>
</tr>
<tr>
<td>CSCuj17827</td>
<td>Withdraw message incompatible with CUCM</td>
</tr>
<tr>
<td>CSCug97383</td>
<td>Switch crashes with EOAM and IP SLA configurations</td>
</tr>
<tr>
<td>CSCtq21722</td>
<td>SNMP crash forced due to an invalid memory block</td>
</tr>
<tr>
<td>CSCtz66347</td>
<td>Executing show tech over SSH session with rekey crashes the router</td>
</tr>
<tr>
<td>CSCuf51357</td>
<td>Cisco IOS SSL VPN Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCuh97409</td>
<td>Input Queue Wedge with DTLS and SSLVPN</td>
</tr>
<tr>
<td>CSCul30483</td>
<td>Router WebVPN Java Plugins fail after upgrade to Java 7 Update 45</td>
</tr>
<tr>
<td>CSCui23099</td>
<td>WOL causes interface wedge on the router interface to etherswitch</td>
</tr>
<tr>
<td>CSCuh09324</td>
<td>udp entries not deleted from flowmgr table</td>
</tr>
<tr>
<td>CSCuj65437</td>
<td>MMOH to PSTN stops streaming when GW receives successive OLCs</td>
</tr>
<tr>
<td>CSCuh57439</td>
<td>Router reloads due to memory exception in checkheaps process</td>
</tr>
<tr>
<td>CSCuj72215</td>
<td>RTCP packets fill up input queue causing performance issues</td>
</tr>
<tr>
<td>CSCue56272</td>
<td>WATCHDOG timeout crash: VOIP_RTP after SYS-3-CPUHOG</td>
</tr>
<tr>
<td>CSCuh87195</td>
<td>Crash with gw-accounting and call-history configured</td>
</tr>
<tr>
<td>CSCug71832</td>
<td>I/O Memory leak - &quot;SCCP Application&quot;</td>
</tr>
<tr>
<td>CSCug22238</td>
<td>UUS/UUI not sent on SIP Invite from a Refer TDM GW</td>
</tr>
<tr>
<td>CSCtz13023</td>
<td>VOICE SIP registrar may crash during registration request</td>
</tr>
<tr>
<td>CSCuh92837</td>
<td>Gateway Won't Initiate Switchover if Fax Tones Detected in Early Media</td>
</tr>
<tr>
<td>CSCui54359</td>
<td>GW failed to switch to t38 v3 fax relay for SG3 calls</td>
</tr>
</tbody>
</table>
### Resolved Bugs—Cisco IOS Release 15.2(4)M5

**Table 7**  
**Resolved Bugs—Cisco IOS Release 15.2(4)M5**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCum86176</td>
<td>GRE keepalive response getting dropped on cellular interface</td>
</tr>
<tr>
<td>CSCu53438</td>
<td>Graceful busyout functionality is not working on gateway as expected</td>
</tr>
<tr>
<td>CSCum02221</td>
<td>Cisco IOS Software BGP DoS Vulnerability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCug24114</td>
<td>CTS env download failed on non seed device after reboot</td>
</tr>
<tr>
<td>CSCug62154</td>
<td>Mk1: High CPU 100% due to TPLUS with tacacs config</td>
</tr>
<tr>
<td>CSCub04965</td>
<td>TCP Session hung causing Packet loss</td>
</tr>
<tr>
<td>CSCuh43252</td>
<td>unable to login and high cpu when authenticating with TACACS</td>
</tr>
<tr>
<td>CSCuh43027</td>
<td>BGP route does not disappear from the RIB</td>
</tr>
<tr>
<td>CSCty77441</td>
<td>xe36: Memory leaks seen after unconfiguring BFD sessions</td>
</tr>
<tr>
<td>CSCuc11958</td>
<td>SIP-400 crashes @hmi_priority_update with FRF12 after SPA reload</td>
</tr>
<tr>
<td>CSCui21061</td>
<td>Disabling CDP on a port-channel deletes FHRP and EIGRP MAC addresses</td>
</tr>
<tr>
<td>CSCud24601</td>
<td>dC4MA2B:ics_cs_negopen_active_port: ERROR seen on SSO in Quad-SUP</td>
</tr>
<tr>
<td>CSCui36394</td>
<td>mlpip is causing the packet to be not short aligned</td>
</tr>
<tr>
<td>CSCug17808</td>
<td>EIGRP not advertising redistributed routes from BGP</td>
</tr>
<tr>
<td>CSCug72891</td>
<td>EIGRP successor loop results in SIA</td>
</tr>
<tr>
<td>CSCuh40275</td>
<td>Very High SNMP Engine utilisation when polling cefFESelectionTable</td>
</tr>
<tr>
<td>CSCue93416</td>
<td>c4ma2b: Startup-config is erased when i copy to nvram and reload on ICS</td>
</tr>
<tr>
<td>CSCts11166</td>
<td>Router is crashing at <code>cce_dp_ipc_save_feature_objects</code></td>
</tr>
<tr>
<td>CSCtrq02528</td>
<td>CSCtr87413Crash while doing 'show ip ips session' at high traffic rate</td>
</tr>
<tr>
<td>CSCuh98328</td>
<td>Waas express crash in waas_smb_negcache_add_entry</td>
</tr>
<tr>
<td>CSCue18443</td>
<td>Subnet mask not sent in authorization request</td>
</tr>
<tr>
<td>CSCuh29716</td>
<td>Calls with FAX caps cause transfer to fail and hung the UDP port on CUBE</td>
</tr>
<tr>
<td>CSCud63146</td>
<td>GETVPN fails to install policies , no int to apply policy</td>
</tr>
<tr>
<td>CSCue88175</td>
<td>No SA's found on interface virtual template1</td>
</tr>
<tr>
<td>CSCub52278</td>
<td>OVLD: DVTI virtual-access interfaces may flap during rekying</td>
</tr>
<tr>
<td>CSCua35161</td>
<td>removing tunnel protection doesn't clear up crypto-map on dmvpn HUB</td>
</tr>
<tr>
<td>CSCug34404</td>
<td>XE38 : RP_Crash seen @ __be_interface_action_remove_old_sadb</td>
</tr>
<tr>
<td>CSCue89779</td>
<td>crypto infra does not support ivrf != fvr for interfaces</td>
</tr>
<tr>
<td>CSCuh46031</td>
<td>Flex VPN - Remote access - different Acct-Session-Id for the same user</td>
</tr>
<tr>
<td>CSCuh93698</td>
<td>IPSEC - Calling-Station-Id not sent in the accounting-request</td>
</tr>
<tr>
<td>CSCui06926</td>
<td>IKEv1 Responder to build CERT based on 'ca trustpoint' from isakmp prof</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCug63839</td>
<td>Memory leak seen in CryptoIKMP process (crypto_ikmp_config_send_ack_addr)</td>
</tr>
<tr>
<td>CSCu78524</td>
<td>Pings near to the size configured as &quot;ppp multilink fragment size&quot; fails</td>
</tr>
<tr>
<td>CSCug7021</td>
<td>SYS-2-BADSHARE Bad refcount in retparticle, ptr=xx, count=0 errors seen</td>
</tr>
<tr>
<td>CSCug31938</td>
<td>Crash when QOS policy with NBAR is applied to ATM using rs8234 Driver</td>
</tr>
<tr>
<td>CSCuh23940</td>
<td>9th port couldn't up for HWIC-D-9ESW</td>
</tr>
<tr>
<td>CSCtz54775</td>
<td>Dynamic MAC addresses not getting learned by forwarding port immediately</td>
</tr>
<tr>
<td>CSCuh54504</td>
<td>Local orig. ping drops on Ge when policy applied to Serial interface</td>
</tr>
<tr>
<td>CSCub83800</td>
<td>Copperopolis Ethernet I/F config removed while loading Ver15.2(4)M1.2</td>
</tr>
<tr>
<td>CSCuf48207</td>
<td>Group (0) info: SHDSL wire-pair (0) is in DSL DOWN state</td>
</tr>
<tr>
<td>CSCue68318</td>
<td>PVC goes down when EIGRP is enabled</td>
</tr>
<tr>
<td>CSCtz98228</td>
<td>Router Crashes when traffic sent from Web Poly-graph tool</td>
</tr>
<tr>
<td>CSCue69214</td>
<td>Memory leak @ __be_fmd_get_if_fn_buffer on removing MLPPP</td>
</tr>
<tr>
<td>CSCud70577</td>
<td>RTSP traffic being dropped with NAT (PAT) and NBAR</td>
</tr>
<tr>
<td>CSCug63013</td>
<td>NHRP multicast mapping stops working after failover and failback</td>
</tr>
<tr>
<td>CSCug38011</td>
<td>router crash after configuring NTP peer</td>
</tr>
<tr>
<td>CSCui07997</td>
<td>OSPF installs multiple sham-link nexthops in RIB</td>
</tr>
<tr>
<td>CSCuh32177</td>
<td>OSPFv3 no passive-int &lt;if-name&gt; incorrectly added for ipv6 int</td>
</tr>
<tr>
<td>CSCue45822</td>
<td>rivendell_oid_sm tracebacks found on c7200p router</td>
</tr>
<tr>
<td>CSCuf56842</td>
<td>Crash after 'show pfr master application detail' command via SSH</td>
</tr>
<tr>
<td>CSCug78098</td>
<td>SUP crash in pimv2_show_rp_hash</td>
</tr>
<tr>
<td>CSCue32707</td>
<td>PKCS12 &quot;crypto pki export&quot; may crash router</td>
</tr>
<tr>
<td>CSCug50606</td>
<td>IPCP: Different pool addresses are assigned for client</td>
</tr>
<tr>
<td>CSCtz19192</td>
<td>Router crash @ pppoe_fast_send_pack and pppoe_fastsend</td>
</tr>
<tr>
<td>CSCuh56327</td>
<td>Crash/Tracebacks occurs with IP SLA Responder on ASR1002</td>
</tr>
<tr>
<td>CSCui14692</td>
<td>IP SLA stacklow or memory corruption crash</td>
</tr>
<tr>
<td>CSCtd45679</td>
<td>Removing ip sla probe (configured by SNMP) in CLI reloads Standby Sup</td>
</tr>
<tr>
<td>CSCud13768</td>
<td>RP crashed while trying to verify UDP-JITTER in IP SLAs vrf-lite</td>
</tr>
<tr>
<td>CSCuh22666</td>
<td>Unexpected reloads due to SNMP Engine CPU HOGs</td>
</tr>
<tr>
<td>CSCug34877</td>
<td>crash during ssh connections establishment / resume</td>
</tr>
<tr>
<td>CSCue74612</td>
<td>Fts Client fails to perform ftp transfer</td>
</tr>
<tr>
<td>CSCud94248</td>
<td>SIP Gateway reloads when it gets 400 error response during Fax upspeed</td>
</tr>
<tr>
<td>CSCuc95160</td>
<td>400 error response when receiving DLCX before sending 200k for CRCX</td>
</tr>
<tr>
<td>CSCue08667</td>
<td>sms not stored - &quot;Running out of buffer for incoming SMS!&quot;</td>
</tr>
<tr>
<td>CSCuh30421</td>
<td>memory leak in X.25 Background XOT SVC possible after CSCtz33622 commit</td>
</tr>
<tr>
<td>CSCue48419</td>
<td>RUDP connection is put on hold and never resumed or reseted</td>
</tr>
</tbody>
</table>
## Open and Resolved Bugs

### Resolved Bugs—Cisco IOS Release 15.2(4)M4

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuc59858</td>
<td>Dynamic-Author should consider src port when detecting retransmissions</td>
</tr>
<tr>
<td>CSCue03316</td>
<td>EoGRE: SSS Manager Segmentation fault/RP reloaded during scale test.</td>
</tr>
<tr>
<td>CSCue18133</td>
<td>[7600] Router crash at show_li_users</td>
</tr>
<tr>
<td>CSCud05636</td>
<td>IPv4 multicast on RBE</td>
</tr>
<tr>
<td>CSCtx07902</td>
<td>Standby RP repeated crash pointing to ipv6_bfd</td>
</tr>
<tr>
<td>CSCuf09006</td>
<td>clear ip bgp * soft out or graceful shut on PE purges all routes on RR</td>
</tr>
<tr>
<td>CSCud55286</td>
<td>On SSO IIF int goes Null &amp; traffic drop,mpvn: 60-90 sec traffic drop</td>
</tr>
<tr>
<td>CSCue76102</td>
<td>XE39:IGBP ipv6_redistributed routes not learned in neighbour router</td>
</tr>
<tr>
<td>CSCua50247</td>
<td>Ping packets dropped between 1501-1524 for NM-16ESW module</td>
</tr>
<tr>
<td>CSCud26339</td>
<td>QoS config change triggers IOSd crash</td>
</tr>
<tr>
<td>CSCub76103</td>
<td>callhome traceback in sending message</td>
</tr>
<tr>
<td>CSCty59104</td>
<td>SNMP set call-home sysStreetAddr using double delimiters cause rpr mode</td>
</tr>
<tr>
<td>CSCue59775</td>
<td>Device crashes when service-policy is removed @ mdb_delete_information</td>
</tr>
<tr>
<td>CSCue48254</td>
<td>Performance degradation on 29xx between 15.0M and 15.2M</td>
</tr>
<tr>
<td>CSCug37242</td>
<td>Memory leak in dialog_set_entity</td>
</tr>
<tr>
<td>CSCtx99353</td>
<td>%SYS-3-INVMEMINT: Invalid memory action error message</td>
</tr>
<tr>
<td>CSCuf93606</td>
<td>3900 series router crashes due to speed dial function.</td>
</tr>
<tr>
<td>CSCua75781</td>
<td>CME reloads for E911 call Elin translation for incoming FXS/FXO trunk</td>
</tr>
<tr>
<td>CSCud95940</td>
<td>CPUHOG &amp; Watchdog at Skinny Msg Server while running CME &amp; Skinny</td>
</tr>
<tr>
<td>CSCub34534</td>
<td>Basic call between 2 SIP Phones over SIP trunk(KPML enabled) fails</td>
</tr>
<tr>
<td>CSCud51791</td>
<td>Memory leak due to CCSIP_SPL_CONTROL process</td>
</tr>
<tr>
<td>CSCue89019</td>
<td>FlexVPN Hub with ISM decapsulate traffic in fvrf instead of ivrf</td>
</tr>
<tr>
<td>CSCug92144</td>
<td>ISAKMP SA negotiation unsuccessful for reventon testcases</td>
</tr>
<tr>
<td>CSCue01721</td>
<td>ISM crashed while clearing crypto sessions at DMVPN hub</td>
</tr>
<tr>
<td>CSCuc45796</td>
<td>ISM crashed while sending ipv4 ping with size 16333</td>
</tr>
<tr>
<td>CSCue66518</td>
<td>ISM-VPN: tlb load/fetch Exception on the ISM</td>
</tr>
<tr>
<td>CSCue53686</td>
<td>ISM: Encryption card consumes fragmented packets</td>
</tr>
<tr>
<td>CSCub59447</td>
<td>rework the bump in the wire vectors for ISM VPN</td>
</tr>
<tr>
<td>CSCub56842</td>
<td>&quot;show cry eli’ active IPSec counters keep increasing lead to VPN failure</td>
</tr>
<tr>
<td>CSCuf61640</td>
<td>%SYS-2-INTSCHED seen when calling random_fill()</td>
</tr>
<tr>
<td>CSCua73191</td>
<td>SSL handshake fails causing browser timeout or Anyconnect package error</td>
</tr>
<tr>
<td>CSCue92705</td>
<td>Address memory leaks in device-sensor for cache delete case.</td>
</tr>
<tr>
<td>CSCug31561</td>
<td>Cisco IOS Software DHCP Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCue62292</td>
<td>%DIALER-6-UNBIND followed by Address Error Crash</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCuc41596</td>
<td>Unable to connect to the remote server with Domain Name</td>
</tr>
<tr>
<td>CSCsr06399</td>
<td>5400XM reloads unexpectedly on stress of xcoding calls with limited DSPs</td>
</tr>
<tr>
<td>CSCud96075</td>
<td>IOS crash due to DSP crash when Transcoder is activated</td>
</tr>
<tr>
<td>CSCud41058</td>
<td>ASR / 152-4.S1 / EIGRP does not read route tags</td>
</tr>
<tr>
<td>CSCtz90697</td>
<td>EIGRP md5 authentication is not working with key id 0</td>
</tr>
<tr>
<td>CSCue26213</td>
<td>EIGRP to BGP redistribution is broken for connected int</td>
</tr>
<tr>
<td>CSCue31321</td>
<td>Crash while running &quot;show ip cef ... detail&quot;</td>
</tr>
<tr>
<td>CSCud86954</td>
<td>Flexible Netflow with DMVPN: Lost cache entry</td>
</tr>
<tr>
<td>CSCuc54300</td>
<td>Standby crashes, Notification timer Expired for RF Client</td>
</tr>
<tr>
<td>CSCud64812</td>
<td>Cisco IOS Software IPv6 VFR Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCuc10588</td>
<td>Crash @ ips_remove_host_entry_from_sis</td>
</tr>
<tr>
<td>CSCue88659</td>
<td>Traceback or crash reported while installing a signature file.</td>
</tr>
<tr>
<td>CSCue75404</td>
<td>Content-Scan: Remove Window Sizing Option towards client and Server</td>
</tr>
<tr>
<td>CSCtx56183</td>
<td>Crash with websense URL filtering configured in</td>
</tr>
<tr>
<td>CSCue71921</td>
<td>Crash after show waas auto-discovery list command is entered</td>
</tr>
<tr>
<td>CSCud86856</td>
<td>Router crash while clearing the ZBF policy-firewall sessions</td>
</tr>
<tr>
<td>CSCud67796</td>
<td>ZBFw SIP ALG - no pregen session for RTP when 180 w/SDP + PRACK w/SDP</td>
</tr>
<tr>
<td>CSCub12694</td>
<td>%SYS-2-INTSCHED: 'may suspend' -Process= &quot;IP SNMP&quot; logs seen</td>
</tr>
<tr>
<td>CSCub71162</td>
<td>Vlan interface is not pingable after netmask change</td>
</tr>
<tr>
<td>CSCue96462</td>
<td>Packets dropped when CEF enabled under Tunnel interface</td>
</tr>
<tr>
<td>CSCue25575</td>
<td>CUBE crashes for SDP pass through +call forward +antitrombone cases</td>
</tr>
<tr>
<td>CSCuf93376</td>
<td>CUBE reloads for EO-EO SDP Passthrough with v6</td>
</tr>
<tr>
<td>CSCue39206</td>
<td>ES Crashes after second 401 Challenge</td>
</tr>
<tr>
<td>CSCub59423</td>
<td>Memory leak @ IPIP channels</td>
</tr>
<tr>
<td>CSCue68761</td>
<td>Buffer leak @ ip_mforward in 15.1(4)M3</td>
</tr>
<tr>
<td>CSCuc25995</td>
<td>Crash with %ALIGN-1-FATAL in IPIsec</td>
</tr>
<tr>
<td>CSCud83835</td>
<td>crypto map on VT with negotiated ip address fails to initiate VPN tunnel</td>
</tr>
<tr>
<td>CSCud88483</td>
<td>GETVPN with IPSEC redundancy: Registration failure on standby GM</td>
</tr>
<tr>
<td>CSCug28904</td>
<td>IKEv2 CRYPTO-4-RECVD_PKT_MAC_ERR with peer nonce length 256 Bytes</td>
</tr>
<tr>
<td>CSCub46423</td>
<td>L2TP/IPSec: Can not connect to HSRP Virtual IP</td>
</tr>
<tr>
<td>CSCue47356</td>
<td>RRI route is leaked when unconfiguring the RRI Static</td>
</tr>
<tr>
<td>CSCue65405</td>
<td>SAs NOT all active after clear crypto gdoi</td>
</tr>
<tr>
<td>CSCub28997</td>
<td>segmentation fault @ __be_wav1_do_walk_threaded with IKEv2</td>
</tr>
<tr>
<td>CSCue77265</td>
<td>XE39: memory leak in aux_msg_acl_destroy_yourself *</td>
</tr>
<tr>
<td>CSCud02391</td>
<td>EIGRP routes are not coming up after removing tunnel interface</td>
</tr>
<tr>
<td>CSCud68178</td>
<td>XE39: DMVPN Hub crashed after physical and tunnel interface flapping</td>
</tr>
<tr>
<td>CSCty26035</td>
<td>Multiple issues, while testing ipsec_ha spt, for ha_test_rekey subtest</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCub93641</td>
<td>Flex-VPN Load Balancing cluster integrity vulnerability</td>
</tr>
<tr>
<td>CSCub93442</td>
<td>FlexVPN Tunnel not coming up when using &quot;ipsec:addrv6 &quot; radius attribute</td>
</tr>
<tr>
<td>CSCuc31761</td>
<td>XE3.9 - KS crashes when removing GDOI groups</td>
</tr>
<tr>
<td>CSCub94825</td>
<td>RRI does not happen in a VRF aware IPSec with stateless HA scenario</td>
</tr>
<tr>
<td>CSCub18622</td>
<td>Auth proxy on 15.x IOS does not apply DACL on tunnel interface</td>
</tr>
<tr>
<td>CSCug34507</td>
<td>Decrypted traffic is process-switched when tunnel is NAT-T udp-encap</td>
</tr>
<tr>
<td>CSCub56064</td>
<td>Ping failed after clearing the crypto isakmp and sa with EZVPN client</td>
</tr>
<tr>
<td>CSCue45934</td>
<td>Return traffic is not coming back in ipv4 session on c6k wit ikev2 MA2re</td>
</tr>
<tr>
<td>CSCuc73473</td>
<td>IPv6 default route is not redistributed in BGP</td>
</tr>
<tr>
<td>CSCua21049</td>
<td>ipv6 route 11::1/128 16::1 multicast fails to insert into murib</td>
</tr>
<tr>
<td>CSCue54104</td>
<td>Crash after 60+ PRI calls are made</td>
</tr>
<tr>
<td>CSCua05196</td>
<td>C2900 crashed at 'cvmx_fpa_shutdown_pool' function due to reload cmd</td>
</tr>
<tr>
<td>CSCue06309</td>
<td>router fails to allocated buffer for different components</td>
</tr>
<tr>
<td>CSCuc70472</td>
<td>PVDM2-DM Modemcap to disable compression works only temporarily</td>
</tr>
<tr>
<td>CSCue52864</td>
<td>3900ePPP Down When O/P Service Policy Is applied on the 3 Channel Groups</td>
</tr>
<tr>
<td>CSCub53380</td>
<td>AsyncPPP Down When O/P Service Policy Is applied on the 3 Channel Groups</td>
</tr>
<tr>
<td>CSCud56450</td>
<td>PPP interfaces drop PPP frames incrementing some error counters</td>
</tr>
<tr>
<td>CSCud65150</td>
<td>Crash after Kron runs a 'TCL script</td>
</tr>
<tr>
<td>CSCue32350</td>
<td>kron crash after deconfiguring the occurance</td>
</tr>
<tr>
<td>CSCuc06307</td>
<td>L2tpv3:Traffic not carried across PW with interworking type IP</td>
</tr>
<tr>
<td>CSCug00841</td>
<td>PW-R does not work properly when using frame-relay as AC</td>
</tr>
<tr>
<td>CSCty57970</td>
<td>Device configured with Web Security with Cisco ScanSafe may crash</td>
</tr>
<tr>
<td>CSCug17820</td>
<td>Random crash of router with L4F managed timers</td>
</tr>
<tr>
<td>CSCud54365</td>
<td>Scansafe socket not closed by reset from client(CSCub85451 rework)</td>
</tr>
<tr>
<td>CSCue28318</td>
<td>Router crashes while executing test aaa command with wrong LDAP config</td>
</tr>
<tr>
<td>CSCug52119</td>
<td>LIS: existing map-cache entry, BGP route introduced, cef keeps lisp enc</td>
</tr>
<tr>
<td>CSCue61691</td>
<td>Mroute shows data mdt switchover but MRIB still shows up the default MDT</td>
</tr>
<tr>
<td>CSCuf28733</td>
<td>Crash seen at ipnat_tcp_alg_dns_translation</td>
</tr>
<tr>
<td>CSCue94880</td>
<td>H323 calls fail with both inside and outside dynamic NAT configs</td>
</tr>
<tr>
<td>CSCud70577</td>
<td>RTSP traffic being dropped with NAT (PAT) and NBAR</td>
</tr>
<tr>
<td>CSCud67105</td>
<td>VA's are not getting deleted in FlexVPN after clearing cache entries</td>
</tr>
<tr>
<td>CSCue81327</td>
<td>C4MA2B : Crash seen while hardware reset on stand-by</td>
</tr>
<tr>
<td>CSCub95285</td>
<td>MF:Syslog messages are not seen after unconfig and config of the server.</td>
</tr>
<tr>
<td>CSCue36197</td>
<td>7600 Router Crashes When Exiting OSPF Helper Mode (RFC 3623)</td>
</tr>
<tr>
<td>CSCue98812</td>
<td>Extra TTY Logging required for Common Criteria certification on IOS/ISRs</td>
</tr>
<tr>
<td>CSCud72625</td>
<td>7200 VSA high CPU due to interrupts and queues at 100%</td>
</tr>
<tr>
<td>CSCue39518</td>
<td>C7200 : VSA : Encryption Failure with IPSec SSO</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCtq12007</td>
<td>VSA - tunnels w. shared stop working after removing protection from one</td>
</tr>
<tr>
<td>CSCud66669</td>
<td>VSA: GRE with TP - Packet is not decrypted into the correct ivrf</td>
</tr>
<tr>
<td>CSCue55739</td>
<td>MC-BR flap due to learn update while writing to DB</td>
</tr>
<tr>
<td>CSts60458</td>
<td>Memory leak in PfR MIB APC in OER Master Contr process</td>
</tr>
<tr>
<td>CSCud64870</td>
<td>ASR1004 hub router crashed after fetching the CRL</td>
</tr>
<tr>
<td>CSCue85737</td>
<td>Show crypto pki certificates cause reload on ASR</td>
</tr>
<tr>
<td>CSCug58617</td>
<td>show run</td>
</tr>
<tr>
<td>CStu88785</td>
<td>system unstable and crashing after upgrade from 12.4(24)T2 to 15.1(4)M1</td>
</tr>
<tr>
<td>CSCue36321</td>
<td>3945e router crash upon configuring ppp mulilink</td>
</tr>
<tr>
<td>CSCuc13992</td>
<td>iosd process crashes due to a segmentation fault at cp_get_option_spec()</td>
</tr>
<tr>
<td>CSCud36208</td>
<td>Multilink ID range to be increased from existing 65535</td>
</tr>
<tr>
<td>CSCub10950</td>
<td>OC3 IM : IOSD crash on doing an IM oir with APS and PPP encap</td>
</tr>
<tr>
<td>CSCug04187</td>
<td>Fixing build breakage due to CSCuf62756</td>
</tr>
<tr>
<td>CSCud64506</td>
<td>HQF failed to clear on misconfigurations with Bandwidth Remaining ratio</td>
</tr>
<tr>
<td>CSCuf62756</td>
<td>Policy-map was detached when change interface bandwidth</td>
</tr>
<tr>
<td>CSCtz53214</td>
<td>REL3.8 VFI_QOS - Target specific clear counters not working</td>
</tr>
<tr>
<td>CSCuf17023</td>
<td>Buffer leaks and interface wedge with malformed traffic</td>
</tr>
<tr>
<td>CSCue40304</td>
<td>could not find some sender in cli o/p of show ip rsvp sender vrf ivrf1</td>
</tr>
<tr>
<td>CSCuf36446</td>
<td>Router crash on &quot;no metadata flow&quot;</td>
</tr>
<tr>
<td>CSCud11078</td>
<td>MA1.3: Crash observed with auto IP SLA probe for ethernet cfm</td>
</tr>
<tr>
<td>CSCuf93964</td>
<td>Fix for CSCty56830 causes buffer overrun</td>
</tr>
<tr>
<td>CSCue65130</td>
<td>cmCallerID in CISCO-MODEM-MGMT-MIB not updated when there is no CallerID</td>
</tr>
<tr>
<td>CSCue68127</td>
<td>I/O block overrun with SSL configured</td>
</tr>
<tr>
<td>CSCud90568</td>
<td>Input queue wedge with SSLVPN DTLS Client Hello</td>
</tr>
<tr>
<td>CSCuc85321</td>
<td>IOS: Crash in SSLVPN session lookup - reoccurrence of CSCtl22435</td>
</tr>
<tr>
<td>CSCue13902</td>
<td>SSLVPN OTP password prompt not presented to user</td>
</tr>
<tr>
<td>CSCud25043</td>
<td>WebVPN enabled gateway crashed on IOS 15.1(4)M5 due to SSLVPN_PROCESS</td>
</tr>
<tr>
<td>CSCug44667</td>
<td>CM tone detector ON irrespective of SG3 fax / modem features disabled</td>
</tr>
<tr>
<td>CSCta80024</td>
<td>string repeat crashes router</td>
</tr>
<tr>
<td>CSCuc02262</td>
<td>Crash seen at tcp_prepare_for_retransmit for IPv4 and IPv6 traffic</td>
</tr>
<tr>
<td>CSCub98623</td>
<td>Interface input buffers(small buff) leak (TCP pkts) after CSCtn39914 fix</td>
</tr>
<tr>
<td>CSCue49632</td>
<td>tcp closes connection for DLSw peer without calling dlsw_tcpd_fini</td>
</tr>
<tr>
<td>CSCud78362</td>
<td>IOS-GW/VXML-GW drops calls after 350 sim calls are setup</td>
</tr>
<tr>
<td>CSCue33313</td>
<td>VXML GW causes ASR No-Input event - Outbound media stream drops</td>
</tr>
<tr>
<td>CSCue69527</td>
<td>Cannot configure more than 95 SCCP controlled FXS ports on VG350</td>
</tr>
<tr>
<td>CStl55445</td>
<td>Cannot insert call history entry for SIP call</td>
</tr>
<tr>
<td>CSCty91566</td>
<td>Memory Leak in CCSIP_SPI_CONTROL</td>
</tr>
</tbody>
</table>
### Open Bugs—Cisco IOS Release 15.2(4)M3

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCue97986</td>
<td>SIP-SIP CUBE - Hung calls after SIP REFER based transfer</td>
</tr>
<tr>
<td>CSCue49424</td>
<td>Crash on bootup when Kron invokes a chat script on a cellular card</td>
</tr>
<tr>
<td>CSCug43453</td>
<td>EHWIC-Global not able to connect to the network after the reload</td>
</tr>
<tr>
<td>CSCud05497</td>
<td>Rarely WCM fails to send configuration to WaasExpress device</td>
</tr>
<tr>
<td>CSCug55040</td>
<td>SP4624: Encounter heart beat timeout issue and modem crash/freeze</td>
</tr>
<tr>
<td>CSCug22606</td>
<td>SP4604: MC7750 ret_val = 15 aftr continuous bearer creation/deletion</td>
</tr>
</tbody>
</table>
# Resolved Bugs—Cisco IOS Release 15.2(4)M3

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCub55790</td>
<td>Cisco Smart Install denial of service vulnerability</td>
</tr>
<tr>
<td>CSCtn16281</td>
<td>Mesh crash on BVI restart by DHCP</td>
</tr>
<tr>
<td>CSCub61009</td>
<td>Spurious at li_ipv4_accesscheck and crash in intercept_ipv4_slow_check</td>
</tr>
<tr>
<td>CSCtz83221</td>
<td>Active RP crash during ATM pvc-in-range config, CLI issue</td>
</tr>
<tr>
<td>CSCub73177</td>
<td>ASR1K crash with Watchdog Process: BGP Router</td>
</tr>
<tr>
<td>CSCud03273</td>
<td>BGP nexthop is not resolved marked inaccessible though route is available</td>
</tr>
<tr>
<td>CSCua75069</td>
<td>BGP PIC: Update/Withdraw are not sent correctly</td>
</tr>
<tr>
<td>CSCub70336</td>
<td>BGP Task crash on bgp hard reset</td>
</tr>
<tr>
<td>CSCua61330</td>
<td>NSF traffic loss during switchover for prefixes with BGP learnt NH</td>
</tr>
<tr>
<td>CSCub86706</td>
<td>XE3.7.1: router crash with BGP HA SSO while switch-over on pE</td>
</tr>
<tr>
<td>CSCub86011</td>
<td>Embedded Event Manager feature missing for VG202, VG204</td>
</tr>
<tr>
<td>CSCub15610</td>
<td>bus error crash at c5510_rx_interrupt.</td>
</tr>
<tr>
<td>CSCua50697</td>
<td>T1 interface behavior inconsistent across WIC Modules</td>
</tr>
<tr>
<td>CSCub61795</td>
<td>%SYS-2-BADSHARE: Bad refcount in retparticle leading to crash</td>
</tr>
<tr>
<td>CSCub67465</td>
<td>Cisco IOS Software Queue Wedge Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCua22789</td>
<td>Embedded Event Manager feature missing for VG202, VG204</td>
</tr>
<tr>
<td>CSCub86128</td>
<td>User-group commands are not present in configuration</td>
</tr>
<tr>
<td>CSCub79590</td>
<td>Mcp_dev: Traceback seen while doing LC oir after applying dmlp configs</td>
</tr>
<tr>
<td>CSCuc07984</td>
<td>Cisco 819 serial interface doesn’t work with many modems at customer site</td>
</tr>
<tr>
<td>CSCub42181</td>
<td>C3900 Voice Gateway Crash when rebooted with &quot;ccm-manager config&quot; enable</td>
</tr>
<tr>
<td>CSCue06116</td>
<td>mgcp/auto-config support on VG350 should be upto max 160 ports</td>
</tr>
<tr>
<td>CSCuc29980</td>
<td>3925 crashes when the IP phones registers to the call manager</td>
</tr>
<tr>
<td>CSCuc24937</td>
<td>SPM and hence crash in ephone_get_phone_type when ephone_array is null</td>
</tr>
<tr>
<td>CSCud67779</td>
<td>Intermittent one way audio issues for call over sip trunk to BACD</td>
</tr>
<tr>
<td>CSCuc07984</td>
<td>Cisco 819 serial interface doesn’t work with many modems at customer site</td>
</tr>
<tr>
<td>CSCuc07984</td>
<td>Cisco 819 serial interface doesn’t work with many modems at customer site</td>
</tr>
<tr>
<td>CSCuc14674</td>
<td>(ISM + ip traffic-export) dropping packets when cef is enable</td>
</tr>
<tr>
<td>CSCub69976</td>
<td>DMVPN - IOS crashes running 152-2.T2</td>
</tr>
<tr>
<td>CSCuc67033</td>
<td>IOS memory corruption crash occurs when ISM-VPN module is enabled</td>
</tr>
<tr>
<td>CSCud34809</td>
<td>ISM module fails to encrypt, but can decrypt</td>
</tr>
<tr>
<td>CSCud90078</td>
<td>ISM no decrypts/ESP forwarded directly with crypto map on two interfaces</td>
</tr>
<tr>
<td>CSCud90078</td>
<td>ISM no decrypts/ESP forwarded directly with crypto map on two interfaces</td>
</tr>
<tr>
<td>CSCud99034</td>
<td>ISM-VPN crypto engine encaps fails in 15.3(1.11)T</td>
</tr>
<tr>
<td>CSCub14145</td>
<td>ISM-VPN Spurious Error command and counters show wrong values.</td>
</tr>
<tr>
<td>CSCud42529</td>
<td>ISM-VPN: router crash when processing IPv6 ICMP packet</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCud74552</td>
<td>ISR G2: ping failure on EHWIC-1GE-SFP-CU w/ ISM-VPN</td>
</tr>
<tr>
<td>CSCuc05631</td>
<td>Tracebacks@ISM-VPN background</td>
</tr>
<tr>
<td>CSCub84471</td>
<td>WAAS Optimized traffic struck in loop when ISM VPN enabled</td>
</tr>
<tr>
<td>CSCud54133</td>
<td>FIPS certification : need continuous random number generator test</td>
</tr>
<tr>
<td>CSCuc40448</td>
<td>sequence of SIP transfer results in no-way audio for hairpinned calls</td>
</tr>
<tr>
<td>CSCug31561</td>
<td>Cisco IOS Software DHCP Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSTx34823</td>
<td>OSPF on demand keeps on bringing up the dialer/ISDN interface</td>
</tr>
<tr>
<td>CSCub15402</td>
<td>VRF is not getting deleted for a long time.</td>
</tr>
<tr>
<td>CSCuc37047</td>
<td>VSS crashes on reconfiguring &quot;ipv6 unicast-forwarding&quot; couple of times</td>
</tr>
<tr>
<td>CSCuc19862</td>
<td>Flexible Netflow on cellular int cause spurious mem access and CPU HOG</td>
</tr>
<tr>
<td>CSCuc50398</td>
<td>Crash seen @ http_proxy_ezvpn_daemon</td>
</tr>
<tr>
<td>CSCud64812</td>
<td>Cisco IOS Software IPv6 VFR Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCtr47084</td>
<td>router crashes at cce_dp_ipc_classify</td>
</tr>
<tr>
<td>CSCuc30630</td>
<td>Installing Cisco SDF release version S650.0 may cause a router to crash</td>
</tr>
<tr>
<td>CSCty82414</td>
<td>IPS: Crash @ ips_dp_feature_action_internal with IPS,FW,Scansafe</td>
</tr>
<tr>
<td>CSCuc12907</td>
<td>Unable to restore the default config from Wexp CLI</td>
</tr>
<tr>
<td>CSCud02361</td>
<td>ZBFW: Sequence no of Spoofed ACK at the receiver is 0X00</td>
</tr>
<tr>
<td>CSCuc01575</td>
<td>removing control-plane config from a capture point leads to crash</td>
</tr>
<tr>
<td>CSCua12317</td>
<td>Configuring object group crashes router</td>
</tr>
<tr>
<td>CSCtu28696</td>
<td>ASR1k RP exception @ rip_process_mgd_timers on clear ip route*</td>
</tr>
<tr>
<td>CSCub45054</td>
<td>OQD Counter issue: Packet Drops seen on mGRE tunnel.</td>
</tr>
<tr>
<td>CSCub96618</td>
<td>[RLS14] db creation failed: XDR updates arrived before parser updates</td>
</tr>
<tr>
<td>CSCub14044</td>
<td>3900 CUBE gateway randomly crashes</td>
</tr>
<tr>
<td>CSCub90459</td>
<td>CUBE consuming 4xx responses when midcall reinvite consumption active</td>
</tr>
<tr>
<td>CSCuc46087</td>
<td>CUBE ignores UPDATE when received before ACKing SIP dialog</td>
</tr>
<tr>
<td>CSCuc42518</td>
<td>Input queue wedge due to RTCP packets</td>
</tr>
<tr>
<td>CSCuc76298</td>
<td>New Active router crashes immediately after switchover with OOD Options</td>
</tr>
<tr>
<td>CSCuc69342</td>
<td>Router crash due to sipSPI_ipip_build_refer</td>
</tr>
<tr>
<td>CSCua93001</td>
<td>c4ma2: Does not receive/listen auto RP announce from PIM peer</td>
</tr>
<tr>
<td>CSCuc19046</td>
<td>Crash in pmt_mrib_delete_entry following &quot;clear ip mroute *&quot;</td>
</tr>
<tr>
<td>CSCua99969</td>
<td>MLD CPU goes high on FHR, RP is located in other router in v6 vrflite</td>
</tr>
<tr>
<td>CSCua91473</td>
<td>crypto_kmi_add_data_to_pylid memory leak at IPSEC key engine process</td>
</tr>
<tr>
<td>CSCuc71706</td>
<td>show run command runs for minutes</td>
</tr>
<tr>
<td>CSCub99756</td>
<td>ASR1K GETVPN GM uses wrong SPI after rekey until old SA expires.</td>
</tr>
<tr>
<td>CSCud59176</td>
<td>Backout CSCub95141 in XE37</td>
</tr>
<tr>
<td>CSCuc36469</td>
<td>CSR-Crash @ __be_crypto_lookup_short_handle during ezvpn tunnel bring up</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCuc93739</td>
<td>EzVPN client with split network does not come UP when IPSEC SA is down</td>
</tr>
<tr>
<td>CSCub95141</td>
<td>FP pending message refs on removing 'crypto local-address loopback'</td>
</tr>
<tr>
<td>CSCud42938</td>
<td>Identi remains at DMAP side even when there are no ipsec sas</td>
</tr>
<tr>
<td>CSTcz94286</td>
<td>Router with ISM-VPN module requires GRE permit entry on outside ACL</td>
</tr>
<tr>
<td>CSCub05907</td>
<td>RRI isn't propagated after failure of a link, when spoke has dual ISP</td>
</tr>
<tr>
<td>CSCud03877</td>
<td>XE371: after volume rekey, ipsec pd flow set soft/hard traffic limit to 0</td>
</tr>
<tr>
<td>CSCuc08061</td>
<td>DMVPN spoke's crypto session was gone after removing, adding tunnel back</td>
</tr>
<tr>
<td>CSCua45206</td>
<td>Hub crashed while removing Stale Cache entry</td>
</tr>
<tr>
<td>CSCuc45528</td>
<td>Incremental leaks at :__b_nhrp_recv_error_indication</td>
</tr>
<tr>
<td>CSCub99778</td>
<td>ASR1K GETVPN GM does not attempt registration after reload interface up</td>
</tr>
<tr>
<td>CSTu54300</td>
<td>fn_VRFAwareGM: KS crashed while running getvpn unconfig script</td>
</tr>
<tr>
<td>CSCuc77704</td>
<td>GETVPN Suite-B: esp-sha2-hmac TEK policy not downloaded to COOP-KS Sec</td>
</tr>
<tr>
<td>CSTcz78943</td>
<td>Crash after configuring a crypto map on a HSRP enabled interface 2</td>
</tr>
<tr>
<td>CSCud06887</td>
<td>IPSec Stateful Failover - SPIs not replicated after first switch</td>
</tr>
<tr>
<td>CSCuc47399</td>
<td>IKEv2-Accounting Wrong values in STOP Records when locally cleared</td>
</tr>
<tr>
<td>CSCub39268</td>
<td>RP crash due to malformed IKEv2 packets</td>
</tr>
<tr>
<td>CSTu02543</td>
<td>EZVPN client address leak due to peer overlap (NAT)</td>
</tr>
<tr>
<td>CSCua31157</td>
<td>One way IPsec traffic after initial isakmp contact deletes budding SA</td>
</tr>
<tr>
<td>CSCuc94687</td>
<td>SHA256 HW crypto support on 890 Platform is missing</td>
</tr>
<tr>
<td>CSCub74272</td>
<td>Crypto Socket goes to closed state causing SA flaps every phase 2 rekey</td>
</tr>
<tr>
<td>CSCub89144</td>
<td>VTI interface is always in up/up state on HSRP standby</td>
</tr>
<tr>
<td>CSCud22222</td>
<td>ISIS IP FRR crash upon interface/neighbor up event</td>
</tr>
<tr>
<td>CSCuc16172</td>
<td>Start-up config being automatically backed-up on C881W-A-K9</td>
</tr>
<tr>
<td>CSTw89123</td>
<td>Crash while configuring ppp multilink fragment-delay</td>
</tr>
<tr>
<td>CSTw78539</td>
<td>2900 GE in 10Mbps: TX ring stuck %ALIGN-3-TRACE at cn_xfr_ge_safe_start</td>
</tr>
<tr>
<td>CSCuc63884</td>
<td>NMI Watchdog Crash on flash_write_data_16bit() during RF Interdev Reload</td>
</tr>
<tr>
<td>CSCua12945</td>
<td>Applying QoS under the serial interface is causing line protocol DOWN</td>
</tr>
<tr>
<td>CSCub82495</td>
<td>Channel-group is going down with NM-8CE1T1-PRI after router reload</td>
</tr>
<tr>
<td>CSCuc73615</td>
<td>Reload CPE with 'dsl-group auto' ALU-SMLT-C-lines does not train</td>
</tr>
<tr>
<td>CSCuc71493</td>
<td>MAP traffic slow down significantly with WAAS Express enabled</td>
</tr>
<tr>
<td>CSCub44898</td>
<td>Scansafe on IOS: Session becomes stale if not closed properly</td>
</tr>
<tr>
<td>CSCud38774</td>
<td>Router get stuck at 100% CPU while doing scale testing with curl-loader</td>
</tr>
<tr>
<td>CSCts75737</td>
<td>Traceback @ swidb_if_index_link_identity on standby RP</td>
</tr>
<tr>
<td>CSCub86319</td>
<td>Router reloads when enable &quot;no cdma modem dm-log enable&quot; cli</td>
</tr>
<tr>
<td>CSCua04049</td>
<td>ASR1K: The EPC capture failed to stop after the initial start</td>
</tr>
<tr>
<td>CSCud33159</td>
<td>C3925: MPLS traffic is Process switched over ATM interface</td>
</tr>
<tr>
<td>CSCua12396</td>
<td>MFIB Linecard Sync Fails across stack in IPV6 Multicast Routing</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCuf28733</td>
<td>Crash seen at ipnat_tcp_alg_dns_translation</td>
</tr>
<tr>
<td>CStt40285</td>
<td>NAT SIP ALG Vulnerability - Possible Router Crash</td>
</tr>
<tr>
<td>CSCud53687</td>
<td>Non-ALG Traffic Incorrectly Classified as ALG Resulting in Session Drop</td>
</tr>
<tr>
<td>CSCuc44438</td>
<td>mem corrupt in ppack load, also NBAR called in SSO of unsupported platfm</td>
</tr>
<tr>
<td>CSCua31934</td>
<td>Crash seen at __be_address_is_unspecified</td>
</tr>
<tr>
<td>CSCuc45115</td>
<td>Crash seen at nhrp_add_static_map</td>
</tr>
<tr>
<td>CSCua46304</td>
<td>Seg fault at __be_nhrp_group_tunnel_qos_apply on flapping tunnel</td>
</tr>
<tr>
<td>CSCuc44629</td>
<td>NTP crash during bootup</td>
</tr>
<tr>
<td>CSCua61201</td>
<td>reload on 7200VXR due to BFD process</td>
</tr>
<tr>
<td>CStx31177</td>
<td>RLS12: RP crash is observed on avl search</td>
</tr>
<tr>
<td>CSCua29095</td>
<td>Spurious memory access while booting 7600 router</td>
</tr>
<tr>
<td>CSCua13848</td>
<td>To address comments of ddts CSCts44393</td>
</tr>
<tr>
<td>CSCub07855</td>
<td>XE37:%SYS-SP-STDDBY-3-VRF_TABLE_INIT_ERROR on the bootup of router</td>
</tr>
<tr>
<td>CSCtw65575</td>
<td>get for ospfv3AreaAggregateTable objects causes router to crash</td>
</tr>
<tr>
<td>CSCub80386</td>
<td>OSPF MANET:Mismatched hello parameters experienced with Relay IPv6 Test</td>
</tr>
<tr>
<td>CSCud27379</td>
<td>WS-SUP720-3B Crashes due to parser component issue</td>
</tr>
<tr>
<td>CSCud46826</td>
<td>7200 VSA: DMVPN Hub stop encrypting due to Invalid SA error</td>
</tr>
<tr>
<td>CSCub17971</td>
<td>GETVPN Adv: No re-registration after switching from hw to sw crypto eng</td>
</tr>
<tr>
<td>CSCtw98200</td>
<td>RIP commands are forcing full VAI on ASR1k</td>
</tr>
<tr>
<td>CSCtz35999</td>
<td>Cisco IOS Software Protocol Translation Vulnerability</td>
</tr>
<tr>
<td>CSCua56802</td>
<td>qos is removed on 2nd SG member on adding sg n hqos on both the members</td>
</tr>
<tr>
<td>CSCuc55346</td>
<td>SNMP MIB cbQosCMDropPkt &amp; cbQosCMDropByte report 0</td>
</tr>
<tr>
<td>CSCuc15695</td>
<td>SNMP polling issue</td>
</tr>
<tr>
<td>CSCuz94902</td>
<td>Memory Allocation Failure when attaching to a Sip-40 LC from Web GUI</td>
</tr>
<tr>
<td>CSCuc55634</td>
<td>IPV6 static route unable to resolve the destination</td>
</tr>
<tr>
<td>CSCuf17023</td>
<td>Buffer leaks and interface wedge with malformed traffic</td>
</tr>
<tr>
<td>CSCua91698</td>
<td>SRST: ephone-type dissapears from running-config</td>
</tr>
<tr>
<td>CSCua64100</td>
<td>Issue in SCTP Receive message</td>
</tr>
<tr>
<td>CSCuc72594</td>
<td>Cisco IOS Software IP Service Level Agreement Vulnerability</td>
</tr>
<tr>
<td>CSCuc82551</td>
<td>Crash in the &quot;SNMP ENGINE&quot; Process Due to rtMonStatsCaptureEntry</td>
</tr>
<tr>
<td>CSCtg82170</td>
<td>IP SLA destination IP/port config changes over a random period of time</td>
</tr>
<tr>
<td>CSCud46314</td>
<td>Crash seen on Cisco Router when polling ciscoEnvMonSupplyStatusDescr MIB</td>
</tr>
<tr>
<td>CSCto87436</td>
<td>%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Proc</td>
</tr>
<tr>
<td>CSCub80710</td>
<td>SSL handshake failure with ASR 3.7</td>
</tr>
<tr>
<td>CSCua82425</td>
<td>Crash due to reload from emm with unsaved config changes</td>
</tr>
<tr>
<td>CSCud31808</td>
<td>tcp receive window (rcvwnd) goes down, and doesn't recover</td>
</tr>
<tr>
<td>CSCub36403</td>
<td>VSS peer reloads for Line-by-Line sync verifying failure</td>
</tr>
</tbody>
</table>
### Table 11: Resolved Bugs—Cisco IOS Release 15.2(4)M2

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCua42104</td>
<td>CUBE with transcoding causes malformed RTCP packets</td>
</tr>
<tr>
<td>CSCuc96631</td>
<td>incoming calls e1r2 stop working n 152-4.M1</td>
</tr>
<tr>
<td>CSCud08595</td>
<td>ISDN Layer 1 Deactivated after reload</td>
</tr>
<tr>
<td>CSCuc12685</td>
<td>Address Error exception with ccTDUtilValidateDataInstance</td>
</tr>
<tr>
<td>CSCua55629</td>
<td>Memory leak in SIPSPI_EV_CC_MEDIA_EVENT</td>
</tr>
<tr>
<td>CSCty61216</td>
<td>Memory leak in CCSIP_SPI_CONTROL</td>
</tr>
<tr>
<td>CSCud01502</td>
<td>Null pointer crash in sipSPIDtmfRelaySipNotifyConfigd</td>
</tr>
<tr>
<td>CSCub19185</td>
<td>Path confirmation fails for SIP call with IPV6 enabled.</td>
</tr>
<tr>
<td>CSCtc17240</td>
<td>SIP: nonce-count 'nc' hex values should be lowercase, RFC compliance</td>
</tr>
<tr>
<td>CSCzt21456</td>
<td>Unexpected reload due to CCSIP_SPI_CONTROL process</td>
</tr>
<tr>
<td>CSCud67792</td>
<td>3G+WiFi ATT SKU of 819 giving &quot;Invalid Modem inserted&quot;</td>
</tr>
<tr>
<td>CSCua65278</td>
<td>Modem disappear with cli &quot;cellular 0 cdma mode evdo&quot;</td>
</tr>
<tr>
<td>CSCuc79143</td>
<td>Cellular Profile Inactive should bring down the Cellular Interface</td>
</tr>
<tr>
<td>CSCud06180</td>
<td>CWAN_SHIM/SDK crash EHWIC-4G-LTE-V</td>
</tr>
<tr>
<td>CSCuc91717</td>
<td>removed x25 translation statement caused router to crash</td>
</tr>
<tr>
<td>CSCub30381</td>
<td>Router crash seen at process_wait_for_event due to x25</td>
</tr>
</tbody>
</table>

---

### Resolved Bugs—Cisco IOS Release 15.2(4)M2

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCua30053</td>
<td>Client failing to authenticate with dot1x authentication</td>
</tr>
<tr>
<td>CSCty74859</td>
<td>ISG PWLAN: Memory leaks@ cpf_get_unbundle_pak_buffer with latest image</td>
</tr>
<tr>
<td>CSCub17985</td>
<td>Memory leak with ppp event</td>
</tr>
<tr>
<td>CSCua01641</td>
<td>NAS-IP address in Accounting-on packet is 0.0.0.0.</td>
</tr>
<tr>
<td>CSCua9947</td>
<td>RP crashes when Framed-IPv6-Route downloaded from freeradius on MLPPP ses</td>
</tr>
<tr>
<td>CSCtk15666</td>
<td>SEC-MAX-LENG: Enforce Maxium Password Length</td>
</tr>
<tr>
<td>CSCua85934</td>
<td>SessProvisioning fail in ISG-SCE interface</td>
</tr>
<tr>
<td>CSCua58100</td>
<td>SYS-2-NOTQ TBs with EAPSIM Roaming at Scale</td>
</tr>
<tr>
<td>CSCtz89334</td>
<td>Traffic blackhole while a single pair of 4wire EFM bond connection down</td>
</tr>
<tr>
<td>CSCua19425</td>
<td>ASR Watchdog Timeout: BGP Router during BFD message servicing</td>
</tr>
<tr>
<td>CSCtz71084</td>
<td>BGP PIC EDGE prefix leak after removal of prefix</td>
</tr>
<tr>
<td>CSCub10951</td>
<td>BGP-DP: Missing updates for inter-cluster BE</td>
</tr>
<tr>
<td>CSCua40790</td>
<td>Incremental leaks at IPToOctetString on polling MIBs on the router</td>
</tr>
<tr>
<td>CSCty89224</td>
<td>IOS crashed when receiving mvpn6 route in BGP update</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCtz44989</td>
<td>Redistribution between two different EIGRPv6 VRF using BGP doesn't work.</td>
</tr>
<tr>
<td>CSCua06598</td>
<td>Router crash when polling inetCidrRouteEntry ipv6 MIB.</td>
</tr>
<tr>
<td>CSCua27852</td>
<td>Traffic loss is seen in pure BGP NSR environment.</td>
</tr>
<tr>
<td>CSCtj59117</td>
<td>%SYS-2-BADSHARE error message is reported on c1801 router.</td>
</tr>
<tr>
<td>CSCtz52843</td>
<td>ATM interface goes down after error messages on 1841.</td>
</tr>
<tr>
<td>CSCua93688</td>
<td>High latency with EHWIC-1GE-SFP-CU.</td>
</tr>
<tr>
<td>CSCits87612</td>
<td>2911 l2tpv3 tunnel shows high latency with EHWIC-1GE-SFP-CU.</td>
</tr>
<tr>
<td>CSCub13317</td>
<td>Cisco 2900 with VWIC2-2MFT-T1/E1: increasing input errors and CRC error.</td>
</tr>
<tr>
<td>CSCub67465</td>
<td>Cisco IOS Software Queue Wedge Denial of Service Vulnerability.</td>
</tr>
<tr>
<td>CSCtz47595</td>
<td>Dial string sends the digits at incorrect times.</td>
</tr>
<tr>
<td>CSCub16372</td>
<td>Very rarely, ISR-G2 IOS cannot boot up with certain ROMMON versions.</td>
</tr>
<tr>
<td>CSCua61814</td>
<td>Overhead accounting configuration changed on XE37 image.</td>
</tr>
<tr>
<td>CSCub19471</td>
<td>Router crash during boot up with masic config.</td>
</tr>
<tr>
<td>CSCtx36095</td>
<td>Mcp_dev: Traceback seen while doing LC oir after applying dmlp configs.</td>
</tr>
<tr>
<td>CSCuc47675</td>
<td>Traffic blackhole when one link is down in EFM bond (CSCtz89334).</td>
</tr>
<tr>
<td>CSCub43088</td>
<td>Delayed UCSE configuration: Wrong module type in slot 2.</td>
</tr>
<tr>
<td>CSCtz58719</td>
<td>Another watchdog timeout in mdb_tree_lookup.</td>
</tr>
<tr>
<td>CSCtw45480</td>
<td>Traffic fails over GRE with self zones configured.</td>
</tr>
<tr>
<td>CSCuc07799</td>
<td>Router (with ISM) crashed upon boot or switch between active/standby.</td>
</tr>
<tr>
<td>CSCuc82992</td>
<td>Router crashed upon execution of &quot;no crypto engine slot 0&quot;.</td>
</tr>
<tr>
<td>CSCua73419</td>
<td>Transform set include SHA2 doesn't work with ISM.</td>
</tr>
<tr>
<td>CSCub28913</td>
<td>VPN-ISM dropping packets for TP encaps’d pkst when crypto map is applied.</td>
</tr>
<tr>
<td>CSCua69657</td>
<td>Traceback seen when executing cli &quot;sh clock detail&quot;.</td>
</tr>
<tr>
<td>CSCua55785</td>
<td>Dialer: Fix build failure in t_base_3.</td>
</tr>
<tr>
<td>CSCua44462</td>
<td>DNS answer is not cached for X25 to IP address resolution.</td>
</tr>
<tr>
<td>CSCua39390</td>
<td>IAD2432 PRI voice port config is removed after the reload 15.1(3)T.</td>
</tr>
<tr>
<td>CSCts55778</td>
<td>EIGRP SAF backward compatibility problem with capabilities-manager.</td>
</tr>
<tr>
<td>CSCsq83006</td>
<td>Port-channel down makes EIGRP SIA.</td>
</tr>
<tr>
<td>CSCua77729</td>
<td>Embedded 801 AP unreachable with reload in command on CISCO1941W.</td>
</tr>
<tr>
<td>CSCua24689</td>
<td>25470DMVPN: fragment sent without label with vfr.</td>
</tr>
<tr>
<td>CSCtq91063</td>
<td>Crash while fragmenting a tunnel packet.</td>
</tr>
<tr>
<td>CSCub54872</td>
<td>fib missing connected interface for interface receive prefix.</td>
</tr>
<tr>
<td>CSCtu07968</td>
<td>ISR 890: Perf mon reports incorrect loss packets/percent with 0 loss.</td>
</tr>
<tr>
<td>CSCtx74051</td>
<td>Unsupported subtraffic bits from XDR not ignored; ISSU downgrade breaks.</td>
</tr>
<tr>
<td>CSCua55797</td>
<td>privilege exec level 0 show glbp brief command causes a MALLOCFAIL.</td>
</tr>
<tr>
<td>CSCtz26735</td>
<td>SDP Process is broken in PI18 (15.2(3)T).</td>
</tr>
<tr>
<td>CSCua97209</td>
<td>NAM CLI analysis-module missing with SRE and Canis.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCsy93069</td>
<td>Crash in L7 DPI after a few hours of telepresence traffic</td>
</tr>
<tr>
<td>CSCub52892</td>
<td>Options log and reset aren't configured in URL filtering policies</td>
</tr>
<tr>
<td>CSCua99687</td>
<td>BFD won't come up if Zone Based Firewall is applied on interface</td>
</tr>
<tr>
<td>CSCtz42421</td>
<td>Crash inspecting h225 with Zone Based Firewalls</td>
</tr>
<tr>
<td>CSCtz59145</td>
<td>Crash while inspecting SIP traffic with Zone Based Firewalls</td>
</tr>
<tr>
<td>CSCtu08373</td>
<td>Various IOS-FW crashes when traffic is sent across router</td>
</tr>
<tr>
<td>CSCtz80643</td>
<td>CEF unresolved and receive adjacency for VAI using VRF PBR selection</td>
</tr>
<tr>
<td>CSCtu28696</td>
<td>ASR1k RP exception @ rip_process_mgd_timers on clear ip route*</td>
</tr>
<tr>
<td>CSCtw52819</td>
<td>OQD: Packet Drops seen on mGRE tunnel.</td>
</tr>
<tr>
<td>CSCua70065</td>
<td>CUBE reloads on testing DO-EO Secure Video Call</td>
</tr>
<tr>
<td>CSCty35726</td>
<td>InterOp:Cube-NavTel : LTI: Video Xcode Call with plain Audio FAILS</td>
</tr>
<tr>
<td>CSCua42523</td>
<td>router crashes and reloads when name-server is ipv4 for dual-stack</td>
</tr>
<tr>
<td>CSCua45122</td>
<td>ipmulticast event trace consumes huge memory on 3k</td>
</tr>
<tr>
<td>CSCtz50204</td>
<td>Crash seen while applying &quot;vrf ivrf2&quot; on Server</td>
</tr>
<tr>
<td>CSCub49291</td>
<td>DMVPN IPv6: Static tunnels failed to build between hub and spokes</td>
</tr>
<tr>
<td>CSCts08224</td>
<td>Expected Inspect ACL/Sessions are not found for most of the protocols,</td>
</tr>
<tr>
<td>CSCtz47309</td>
<td>FlexVPN: smart defaults: SA negotiation fails due to mismatched mode</td>
</tr>
<tr>
<td>CSCua21166</td>
<td>IOS IPSec Tunnel CERM Count leak</td>
</tr>
<tr>
<td>CSCub07673</td>
<td>ipsec session doesn’t cm up for spa-ipsec-2g if ws-ipsec3 is also present</td>
</tr>
<tr>
<td>CSCua37898</td>
<td>MA2: Memory leak seen @ crypto_ss_enable_ipsec_profile on VSS</td>
</tr>
<tr>
<td>CSCua21201</td>
<td>RP2 reloaded in 8k tunnel overnight traffic test</td>
</tr>
<tr>
<td>CSCtz86763</td>
<td>Session/Memroy leak in Crypto SS Process on session churn</td>
</tr>
<tr>
<td>CSCtz90984</td>
<td>Switch crashes when trying to enable IPSec md5 authentication on the SVI</td>
</tr>
<tr>
<td>CSCty03133</td>
<td>XE35: Memory leak in IPSEC key engine process</td>
</tr>
<tr>
<td>CSCtz73836</td>
<td>NHRP crash due to DMVPN event-trace</td>
</tr>
<tr>
<td>CSCub07382</td>
<td>FlexVPN: Spoke to Spoke : NHRP cache entry expires even with traffic</td>
</tr>
<tr>
<td>CSCtz72390</td>
<td>FlexVPN: authorization by name mangler fails silently w/ diag traceback</td>
</tr>
<tr>
<td>CSCua39107</td>
<td>iprib_first_hop not returning NHO route added by NHRP</td>
</tr>
<tr>
<td>CSCub42920</td>
<td>GETVPN: KS fails to validate hash in rekey ACK from previous GM versions</td>
</tr>
<tr>
<td>CSCua10556</td>
<td>crypto ikev2 sa stuck in delete state</td>
</tr>
<tr>
<td>CSCua28346</td>
<td>IKEV2 RSA- Crash in ikev2_ios_mib_tunnel_stop during rekey</td>
</tr>
<tr>
<td>CSCua51991</td>
<td>Inconsistency for IPSec SA count between IKEv2 and IPSec PI database</td>
</tr>
<tr>
<td>CSCua56184</td>
<td>RP crashes during flexvpn longevity after multiple RP switchovers</td>
</tr>
<tr>
<td>CSCtx85623</td>
<td>ATM Output Queue Stuck (HWIC-1ADSL)</td>
</tr>
<tr>
<td>CSCtx39953</td>
<td>kron policy multiple telnet cause crash</td>
</tr>
<tr>
<td>CSCua78468</td>
<td>L4F crash on 3945e with scansafe - Traffic Codenomicon</td>
</tr>
<tr>
<td>CSCub85451</td>
<td>Scansafe socket not closed by reset from client</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCtz36906</td>
<td>Alignment corrections at les_return_src_mac_ptr; high CPU seen</td>
</tr>
<tr>
<td>CSCua19933</td>
<td>Crash at mace_dp_add_or_remove_from_feature_path on removing mace</td>
</tr>
<tr>
<td>CSCub51862</td>
<td>Crash seen at mace_dp_hash_table_destroy</td>
</tr>
<tr>
<td>CSCub58932</td>
<td>MACE Export timing getting out of sync after a week</td>
</tr>
<tr>
<td>CSCtz01079</td>
<td>router crash when I enabled uri stats with one http request</td>
</tr>
<tr>
<td>CSCub62116</td>
<td>Spurious memory access at mace_dp_feature_action_pre_waas</td>
</tr>
<tr>
<td>CSCty65189</td>
<td>First PIM Reg message gets dropped by ZBFW</td>
</tr>
<tr>
<td>CSCua86620</td>
<td>Metadata App-ID for vmware incorrect</td>
</tr>
<tr>
<td>CSCua63440</td>
<td>Metadata crash @ be_fmd_lfid_show_entry_for_id</td>
</tr>
<tr>
<td>CSCua18166</td>
<td>Need to support sub-app-id</td>
</tr>
<tr>
<td>CSCtz50683</td>
<td>adj not freed upon removing replication client</td>
</tr>
<tr>
<td>CSCua40273</td>
<td>Crash at mplsvpnmb_get_vrf_interface_info</td>
</tr>
<tr>
<td>CSCtw72952</td>
<td>Path protection not working once primary path is deleted</td>
</tr>
<tr>
<td>CSCua96106</td>
<td>MSP subsystems are not included in 890 packaging</td>
</tr>
<tr>
<td>CSCto88178</td>
<td>Double / Twice NAT Corrupts H.323 Control Packets</td>
</tr>
<tr>
<td>CSCua62545</td>
<td>attributes are not getting exported correct, change using attribute-set</td>
</tr>
<tr>
<td>CSCua78555</td>
<td>custom protocols not retaining attributes upon pp load</td>
</tr>
<tr>
<td>CSCua70158</td>
<td>Nbar fails to recognize traffic in the match protocol http url/host</td>
</tr>
<tr>
<td>CSCua47570</td>
<td>Observing rp crash @ ospfv3_show_event_data_rib</td>
</tr>
<tr>
<td>CSCtx66046</td>
<td>OSPF NSR: Stby crashes @ _be_db_free_check</td>
</tr>
<tr>
<td>CSCua96354</td>
<td>Crash after 'show oer master traffic-class performance' command</td>
</tr>
<tr>
<td>CSCub91815</td>
<td>Authentication with valid certificate fails on spoke-to-spoke DMVPN</td>
</tr>
<tr>
<td>CSCua71038</td>
<td>Crash while checking OCSP certificate status and CRL chaching</td>
</tr>
<tr>
<td>CSCtz37164</td>
<td>ASR1K re-transmits IPCP Author. Access-Request after session closed</td>
</tr>
<tr>
<td>CSCua84923</td>
<td>ASR fail to attach a Cos Policy following changes on Shaping Config</td>
</tr>
<tr>
<td>CSCtw88689</td>
<td>crash seen with 3900e platform</td>
</tr>
<tr>
<td>CSCty86039</td>
<td>crash seen with @ hqf_restore_pak</td>
</tr>
<tr>
<td>CSCua67998</td>
<td>Dialer:crashed @ hqf_restore_pak</td>
</tr>
<tr>
<td>CSCtz13465</td>
<td>High CPU on Enhanced flexwan Module - rework CSCtu09859</td>
</tr>
<tr>
<td>CSCtz61599</td>
<td>Port-channel11 has more than one active member link</td>
</tr>
<tr>
<td>CSCub46570</td>
<td>Rework CSCua84923 for compiling issue</td>
</tr>
<tr>
<td>CSCtz71171</td>
<td>Subscriber drops not reported in mod4 accounting</td>
</tr>
<tr>
<td>CSCua19207</td>
<td>XE37: not able to apply sub-int shape + tunnel QoS from 5/25</td>
</tr>
<tr>
<td>CSCua21171</td>
<td>xe37: Some of the bundles in dlfioatm sessions are not pingable</td>
</tr>
<tr>
<td>CSCua97981</td>
<td>IOS redundancy slow to come up and gets stuck in final progression</td>
</tr>
<tr>
<td>CSCtz58941</td>
<td>Crash show_network after multiple times &quot;show ip route x&quot; cmd executed</td>
</tr>
<tr>
<td>CSCua23217</td>
<td>Controllers not coming up when CPE is in AUTO mode for ATM</td>
</tr>
</tbody>
</table>
### Open and Resolved Bugs

**Resolved Bugs—Cisco IOS Release 15.2(4)M1**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCub04345</td>
<td>Memory leak after applying ip sla-path-echo and path-jitter config</td>
</tr>
<tr>
<td>CSCub33470</td>
<td>Multiple &quot;ip sla read&quot; CLI shows up by default on loading nightly</td>
</tr>
<tr>
<td>CSCtz40460</td>
<td>Crash or hang on router running sslvpn</td>
</tr>
<tr>
<td>CSCub39124</td>
<td>IOS WebVPN &quot;SSL Cookie Not Used&quot; Hardening</td>
</tr>
<tr>
<td>CSCub47910</td>
<td>ssl-vpn: Unexpected exception to CPU: vector D</td>
</tr>
<tr>
<td>CSCua60100</td>
<td>Crash seen at &quot;ip_acl_peruser_ctx_free&quot; while clearing the session</td>
</tr>
<tr>
<td>CSCua48060</td>
<td>Router gets reloaded after applying the ppp &amp; aaa authentication</td>
</tr>
<tr>
<td>CSCub85754</td>
<td>Inception DSL Cannot Ping in VDSL over POTS Mode with Firmware 37hv</td>
</tr>
<tr>
<td>CSCtx80535</td>
<td>DHCP pool with ODAP assigns the same IP to multiple sessions</td>
</tr>
<tr>
<td>CSCub45809</td>
<td>Providing a CLI Knob for handling media loops in Voip RTP</td>
</tr>
<tr>
<td>CSCuc56259</td>
<td>Voice Gateway May Crash Due To %VOIP_RTP-6-MEDIA_LOOP:</td>
</tr>
<tr>
<td>CSCua07791</td>
<td>CCSIP_SPI_CONTRO mem leak at sipSPI_ipip_update_forked_dialog_remote_tag</td>
</tr>
<tr>
<td>CSCua15003</td>
<td>SIP Call CANCEL leak Transcoder resource used on CUBE</td>
</tr>
<tr>
<td>CSCub91111</td>
<td>All outgoing packets are dropped with 3.7G MC8705(firmwareT3.5.3.2)</td>
</tr>
<tr>
<td>CSCuc37365</td>
<td>Bandwidth command is broken under the cellular interface</td>
</tr>
<tr>
<td>CSCua32379</td>
<td>ASR1k Hubs crashed at crypto_ss_set_ipsec_parameters</td>
</tr>
<tr>
<td>CSCtx75071</td>
<td>Publish the crypto_engine changes of CSCty98523 t_base_2</td>
</tr>
<tr>
<td>CSCua49764</td>
<td>Https created WExp certificate - WExp went to offline after upgrade</td>
</tr>
<tr>
<td>CSCub34396</td>
<td>Traffic flow in dmvpn is flowing unencrypted</td>
</tr>
</tbody>
</table>

**Open Bugs—Cisco IOS Release 15.2(4)M**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtw73696</td>
<td>Crash in parser code related to an Exec session</td>
</tr>
<tr>
<td>CSCtz88796</td>
<td>GRE shaping cause packet loss/delay on Special-Services-Engine interface</td>
</tr>
<tr>
<td>CSCtx55113</td>
<td>EHWIC-1GE-SFP-CU - TX Stuck - stops transmitting traffic</td>
</tr>
<tr>
<td>CSCua04185</td>
<td>NM-1T3E3 generates crc/input errors on 29xx for 64 byte traffic</td>
</tr>
<tr>
<td>CSCua50247</td>
<td>Ping packets dropped between 1501-1524 for NM-16ESW module</td>
</tr>
<tr>
<td>CSCty27687</td>
<td>3900 core dumps show up as corrupt when loaded in GDB</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCtz47595</td>
<td>dial string sends the digits at incorrect times</td>
</tr>
<tr>
<td>CSCth20872</td>
<td>%C870_FE-3-TXERR: error messages and reset of Fa interface on 877 router</td>
</tr>
<tr>
<td>CSCua23764</td>
<td>up14b ComplexQoS 362: 10% perf throughput degradation with 15.2(3.14)T</td>
</tr>
<tr>
<td>CSCtz58719</td>
<td>Another watchdog timeout in mdb_tree_lookup</td>
</tr>
<tr>
<td>CSCua04722</td>
<td>crash at qos_update_class_grp_acl</td>
</tr>
<tr>
<td>CSCua76337</td>
<td>Watchdog Crash due to &quot;no [ACL entry number]&quot;</td>
</tr>
<tr>
<td>CSCty19798</td>
<td>3925 router crash with memory corruption</td>
</tr>
<tr>
<td>CSCtx37569</td>
<td>Call Park in CME with BLF intermediately leave Monitor button red</td>
</tr>
<tr>
<td>CSCua75781</td>
<td>CME reloads for E911 call Elin translation for incoming FXS/FXO trunk</td>
</tr>
<tr>
<td>CSCtz81595</td>
<td>AnyConnect on Mac 3.0.07059 and later don't work with Cisco IOS Routers</td>
</tr>
<tr>
<td>CSCtq23960</td>
<td>ISR series routers using PPC or MIPS arch crash &amp; gen empty crash files</td>
</tr>
<tr>
<td>CSCua33158</td>
<td>ISR:IPv6 ping does not work</td>
</tr>
<tr>
<td>CSCua38876</td>
<td>Crash after VPN_HW-1-PACKET_ERROR</td>
</tr>
<tr>
<td>CSCtr63128</td>
<td>Freescale based routers crash at adj_switch_ipv4_generic_les</td>
</tr>
<tr>
<td>CSCua59544</td>
<td>IOS: High CPU while downloading via AC and IOS as headend</td>
</tr>
<tr>
<td>CSCua73191</td>
<td>SSL handshake fails causing browser timeout or Anyconnect package error</td>
</tr>
<tr>
<td>CSCua53874</td>
<td>Router running as voice gateway reset during conferencing</td>
</tr>
<tr>
<td>CSCtz15274</td>
<td>%FLEXDSPRM-3-UNSUPPORTED_CODEC: codec cisco is not supported on dsp T38</td>
</tr>
<tr>
<td>CSCua39390</td>
<td>IAD2432 PRI voice port config is removed after the reload 15.1(3)T</td>
</tr>
<tr>
<td>CSCua72019</td>
<td>AP802GN Radio Shuts Down</td>
</tr>
<tr>
<td>CSCth71093</td>
<td>Core Dump Fails w/ &quot;exception flash all flash:&quot; if Flash Size is &gt;2GB</td>
</tr>
<tr>
<td>CSCtr47084</td>
<td>router crashes at cce_dp_ipc_classify</td>
</tr>
<tr>
<td>CSCtx66904</td>
<td>Router hang / crash while inspecting H.323 traffic</td>
</tr>
<tr>
<td>CSCua72801</td>
<td>IPS + WAAS Inconsistent Behavior</td>
</tr>
<tr>
<td>CSCty82414</td>
<td>IPS: Crash @ ips_dp_feature_action_internal with IPS,FW,Scansafe</td>
</tr>
<tr>
<td>CSCtx56183</td>
<td>Crash with websense URL filtering configured in</td>
</tr>
<tr>
<td>CSCtz28855</td>
<td>IOS URLF: Crash in fw_dp_urlf_http_inspect_control_stream2</td>
</tr>
<tr>
<td>CSCtu08373</td>
<td>Various IOS-FW crashes when traffic is sent across router</td>
</tr>
<tr>
<td>CSCty47860</td>
<td>7200: Same /32 IP has been assigned to multiple VTIs in same VRF.</td>
</tr>
<tr>
<td>CSCua63087</td>
<td>2800: bus error on ACL</td>
</tr>
<tr>
<td>CSCtx72992</td>
<td>GRE Tunnel output is suddenly stuck</td>
</tr>
<tr>
<td>CSCtx23421</td>
<td>Heavy memory leaks with scaled IP SLA configs on DMVPN spoke</td>
</tr>
<tr>
<td>CSCtz84873</td>
<td>Crash due to stack overflow: CCSIP_SPI_CONTROL running low, 0/60000</td>
</tr>
<tr>
<td>CSCua70065</td>
<td>CUBE reloads on testing DO-E0 Secure Video Call</td>
</tr>
<tr>
<td>CSCua42523</td>
<td>router crashes and reloads when name-server is ipv4 for dual-stack</td>
</tr>
<tr>
<td>CSCtz47309</td>
<td>FlexVPN: smart defaults: SA negotiation fails due to mismatched mode</td>
</tr>
<tr>
<td>CSCua21166</td>
<td>IOS IPSec Tunnel CERM Count leak</td>
</tr>
</tbody>
</table>
**Resolved Bugs—Cisco IOS Release 15.2(4)M**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtu54300</td>
<td>fn_VRFAwareGM: KS crashed while running getvpn unconfig script</td>
</tr>
<tr>
<td>CSCtu02543</td>
<td>EZVPN client address leak due to peer overlap (NAT)</td>
</tr>
<tr>
<td>CSCua31157</td>
<td>One way IPsec traffic after initial isakmp contact deletes budding SA</td>
</tr>
<tr>
<td>CSCtz84199</td>
<td>DMVPN Spoke crash at __be_crypto_check_acl with traffic going through</td>
</tr>
<tr>
<td>CSCtw89123</td>
<td>Crash while configuring ppp multilink fragment-delay</td>
</tr>
<tr>
<td>CSCua05196</td>
<td>C2900 crashed at 'cvmx_fpa_shutdown_pool' function due to reload cmd</td>
</tr>
<tr>
<td>CSCtz54775</td>
<td>Dynamic MAC addresses not getting learned by forwarding port immediately</td>
</tr>
<tr>
<td>CSCua12945</td>
<td>Applying_QoS under the serial interface is causing line protocol DOWN</td>
</tr>
<tr>
<td>CSCtx52157</td>
<td>CISCO3925E / 2 routers are not communicating behind 2 switches</td>
</tr>
<tr>
<td>CSCtx39953</td>
<td>kron policy multiple telnet cause crash</td>
</tr>
<tr>
<td>CSCua61097</td>
<td>WAAS Express sending corrupt frames to WAAS causing conn resets</td>
</tr>
<tr>
<td>CSCtt40285</td>
<td>NAT SIP ALG Vulnerability - Possible Router Crash</td>
</tr>
<tr>
<td>CSCua70158</td>
<td>Nbar fails to recognize traffic in the match protocol http url/host</td>
</tr>
<tr>
<td>CSCua29351</td>
<td>Crash at nhrpSnmpCompareNodes</td>
</tr>
<tr>
<td>CSCua71038</td>
<td>Crash while checking OCSP certificate status and CRL chaching</td>
</tr>
<tr>
<td>CSCtz59999</td>
<td>Cisco IOS Software Protocol Translation Vulnerability</td>
</tr>
<tr>
<td>CSto08904</td>
<td>Multiple RTP probe operation results in failures - inconsistent results.</td>
</tr>
<tr>
<td>CSCtw80814</td>
<td>Crash while disconnecting SSH session</td>
</tr>
<tr>
<td>CSCtz40460</td>
<td>Crash or hang on router running sslvpn</td>
</tr>
<tr>
<td>CSCua69346</td>
<td>memory leak SSLVPN_PROCESS in processor pool</td>
</tr>
<tr>
<td>CSCua60100</td>
<td>Crash seen at &quot;ip_acl_peruser_ctxt_free&quot; while clearing the session</td>
</tr>
<tr>
<td>CSCua48060</td>
<td>Router gets reloaded after applying the ppp &amp; aaa authentication</td>
</tr>
<tr>
<td>CSCua75666</td>
<td>DSP(pvdm3): Dsp programming failed result in DSP Timeout event 0x12C</td>
</tr>
<tr>
<td>CSCts53278</td>
<td>STE Secure Voice Quality Issue - SCIP line quality set to LOW</td>
</tr>
<tr>
<td>CSCua43850</td>
<td>V110 dialout calls not happening with [VIC2-2BRI-NT/TE with TA]</td>
</tr>
<tr>
<td>CSty91566</td>
<td>Memory Leak in CCSIP_SPI_CONTROL</td>
</tr>
<tr>
<td>CSCtz57013</td>
<td>UC540 crashes randomly every few weeks while running 15.1(2)T4</td>
</tr>
<tr>
<td>CSCty09784</td>
<td>SS7 link does not come up</td>
</tr>
<tr>
<td>CSCua65278</td>
<td>Modem disappear with cli &quot;cellular 0 cdma mode evdo&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtx99544</td>
<td>Exception when no aaa accounting system default vrf VRF3</td>
</tr>
<tr>
<td>CSCtx31175</td>
<td>Framed-IP-Address added twice in accounting STOP record by ISGv4</td>
</tr>
</tbody>
</table>
### Open and Resolved Bugs

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtx95339</td>
<td>ID leak while flapping walkby converted sessions in radius_parse_respons</td>
</tr>
<tr>
<td>CSCtx63545</td>
<td>ISG crash with RP sessions when all radius servers are DEAD</td>
</tr>
<tr>
<td>CSCtw86212</td>
<td>ISG failing to support Radius Attribute filter configuration</td>
</tr>
<tr>
<td>CSCtz5380</td>
<td>ISG: creating invalid radius request packets during retransmission</td>
</tr>
<tr>
<td>CSCtw94598</td>
<td>Reported to RADIUS NAS Port type is changed from Ethernet to Async</td>
</tr>
<tr>
<td>CSCtx51420</td>
<td>RP crash just after boot on 15.2(02)S image nightly dated 14th jan</td>
</tr>
<tr>
<td>CStu34207</td>
<td>SessProvisioning fail in ISG-SCE interface after upgrade to 15.1</td>
</tr>
<tr>
<td>CStu87070</td>
<td>TACACS Enable login with wrong source ip address</td>
</tr>
<tr>
<td>CSty58241</td>
<td>Unexpected response increasing after change on radius host command</td>
</tr>
<tr>
<td>CSua38881</td>
<td>Router reloads @ clear_dspm_counter_per_bay</td>
</tr>
<tr>
<td>CStq17444</td>
<td>A Cisco router may crash after a trunk call is made</td>
</tr>
<tr>
<td>CSCtz2521</td>
<td>Need to allow configuration ofBFD min multiplier to be set to value of 2</td>
</tr>
<tr>
<td>CStq24557</td>
<td>BGP import processing trying to free already freed chunk, causing crash.</td>
</tr>
<tr>
<td>CSCtt35379</td>
<td>BGP Processing Enhancements</td>
</tr>
<tr>
<td>CSty58300</td>
<td>BGP Processing Enhancements</td>
</tr>
<tr>
<td>CSCts79211</td>
<td>BGP RT constraint filters not advertised after SSO switchover</td>
</tr>
<tr>
<td>CSCty03745</td>
<td>BGP sending wrong next-hop while using vplS AD with default route</td>
</tr>
<tr>
<td>CStq95384</td>
<td>BGP still holding memory even after removal in scale NSR scenario</td>
</tr>
<tr>
<td>CSCty96052</td>
<td>Extreme corner case: Crash during BGP scanner process run</td>
</tr>
<tr>
<td>CSCtz13818</td>
<td>IOS not sending refreshed updates to peer after change in route-map</td>
</tr>
<tr>
<td>CSCty78435</td>
<td>MPLSomGRE: match statement ignored in route-map</td>
</tr>
<tr>
<td>CSCtx67474</td>
<td>upd sent with empty nlri when msg consist of 2byte ASpath &amp; 4byte AGGR</td>
</tr>
<tr>
<td>CStt61762</td>
<td>IPV6 multicast frames are not forwarded between ports on EHWIC-*ESG</td>
</tr>
<tr>
<td>CSCty14375</td>
<td>False Temperature alarm in 2911 %ENVMON-1-WARN_HDD_HIGH_TEMP:</td>
</tr>
<tr>
<td>CSCtx64684</td>
<td>ISIS not coming up on the SVI interface of EHWIC-xESG</td>
</tr>
<tr>
<td>CSty96597</td>
<td>Unable to power-cycle modem using test CLI</td>
</tr>
<tr>
<td>CSCtx86674</td>
<td>vpl/vci not coming up after upgrade</td>
</tr>
<tr>
<td>CSCtz70938</td>
<td>3945E crashes when deferred commands applied to SM-SRE-710-K9</td>
</tr>
<tr>
<td>CStw62213</td>
<td>IPSLA Responder reports excessive packet drops on c3900e</td>
</tr>
<tr>
<td>CSCtx49098</td>
<td>Crash at udb_pre_feature_unbind_cleanup on manipulating QoS policy</td>
</tr>
<tr>
<td>CSCty15615</td>
<td>Either only one direction p-map seen after detaching another a p-map</td>
</tr>
<tr>
<td>CSCtq27016</td>
<td>Qos related Memory leak is observed on ES-40</td>
</tr>
<tr>
<td>CSCty73817</td>
<td>RP SWO fails with qos enabled on 12K PTA PPPoE sessions</td>
</tr>
<tr>
<td>CSCty24707</td>
<td>Standby RP keeps rebooting with %QOS-3-HA_BULK_SYNC_BEFORE_TIMEOUT</td>
</tr>
<tr>
<td>CSCty34020</td>
<td>i82545/i82546 ring-check algorithm(test cli) disabled after hang</td>
</tr>
<tr>
<td>CSCtz08388</td>
<td>866VAE_ADSL2+/ADSL2 cannot train up after config change on DSLAM side</td>
</tr>
<tr>
<td>CSCua16561</td>
<td>c88x HW-crypto - wrong ESP next header field for jumbo-sized packets</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCua08876</td>
<td>LCP: O PROTREJ [Open] id 2 len 20 protocol IPV6CP on 867VAE</td>
</tr>
<tr>
<td>CSCtz70623</td>
<td>Shutting G.SHDSL interface causes router to crash</td>
</tr>
<tr>
<td>CSCtz05090</td>
<td>SRTG NX-ROMMON security enhancement: c880, c1800, uc500</td>
</tr>
<tr>
<td>CSCty01234</td>
<td>Unexpected reboot due to Sigtrap Exception on applying qos pre-classify</td>
</tr>
<tr>
<td>CSCtx22322</td>
<td>When installing IRQ0 set the PIC to be at same level for c800 platforms</td>
</tr>
<tr>
<td>CSCua50490</td>
<td>IOS ucse configs not pushed automatically to BMC after module oir</td>
</tr>
<tr>
<td>CSCty07771</td>
<td>Backout CSCts55654</td>
</tr>
<tr>
<td>CSCty86111</td>
<td>Router crashed after &quot;no ccm-manager falback-mgep&quot; command was entered.</td>
</tr>
<tr>
<td>CSCtd43540</td>
<td>Memory leak due to CDP process</td>
</tr>
<tr>
<td>CSCtw59338</td>
<td>MTRACE and crash following on switch using CDP</td>
</tr>
<tr>
<td>CSCtx86116</td>
<td>ZBFW-HA: ACTIVE router crashing when HA config is removed</td>
</tr>
<tr>
<td>CSCtw78064</td>
<td>Display Logout message is not cleared, when user logged out from EM</td>
</tr>
<tr>
<td>CSCtz12714</td>
<td>Router crashes after CBarge event</td>
</tr>
<tr>
<td>CSCty64721</td>
<td>Improper memory allocation by CTI process crashing CME</td>
</tr>
<tr>
<td>CSCty59692</td>
<td>CME is crashing with SNR + CFNA on SNR mobile</td>
</tr>
<tr>
<td>CSCty25963</td>
<td>CME reloads on configuring no mode cme under voice register global</td>
</tr>
<tr>
<td>CSCty18156</td>
<td>CUCME is Crashing while invoking extension mobility from SIP Phone</td>
</tr>
<tr>
<td>CSCtw67283</td>
<td>Unexpected exception to CPU in action_add_standard_global during traffic</td>
</tr>
<tr>
<td>CSCtz15211</td>
<td>15.ISM: Double encryption failure</td>
</tr>
<tr>
<td>CSCty98834</td>
<td>gm crash due to ISM VPN engine leaking memory</td>
</tr>
<tr>
<td>CSCua17746</td>
<td>IKEv2 session fails with VSA and ISM VPN modules after CSCtn72884</td>
</tr>
<tr>
<td>CSCtz25364</td>
<td>ISM VPN and ASR1k GETVPN TBAR cannot interoperate packet drops</td>
</tr>
<tr>
<td>CSCtz51773</td>
<td>ISM-VPN crashing due to an assert in IPSec classification code</td>
</tr>
<tr>
<td>CSCua45685</td>
<td>ISM-VPN: Group Member Crashes when handling GETVPN Rekey.</td>
</tr>
<tr>
<td>CSCty54434</td>
<td>ISRG2 w/ ISM VPN fails to initiate multiple tunnels</td>
</tr>
<tr>
<td>CSCty65334</td>
<td>unconfig cry acl cause crash in c3900 router with ISM crypro engine.</td>
</tr>
<tr>
<td>CSCts37446</td>
<td>c7600: traceback seen @ zamboni_create_flow_cmd</td>
</tr>
<tr>
<td>CSCty44281</td>
<td>Commit shimming changes related to hw source entropy</td>
</tr>
<tr>
<td>CSCtz95782</td>
<td>Packet drop on crypto engine with Buffer Unavailable if QoS is applied</td>
</tr>
<tr>
<td>CSCt94440</td>
<td>RLS3.6 eToken: RP reloaded when issue &quot;show cryp eli all&quot; with IKEv2</td>
</tr>
<tr>
<td>CSCty42626</td>
<td>RSA operations fail with 'malloc' at interrupt level' msg</td>
</tr>
<tr>
<td>CSCtx82775</td>
<td>Software MTP leakon ASR resulting in hung calls</td>
</tr>
<tr>
<td>CSCty96049</td>
<td>DHCP Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCtj48387</td>
<td>Crash on ASR due to corrupt values passed from DHCP component</td>
</tr>
<tr>
<td>CSCtx71185</td>
<td>Crash due to uninitialized fastsend vector in Dialer HWIDB</td>
</tr>
<tr>
<td>CSCts00341</td>
<td>CLI requiring DNS lookup cannot be configured when in SSO mode</td>
</tr>
<tr>
<td>CSCua44462</td>
<td>DNS answer is not cached for X25 to IP address resolution</td>
</tr>
</tbody>
</table>
## Open and Resolved Bugs

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtx61557</td>
<td>Crash after authc result 'success' from 'dot1x' for client (Unknown MAC)</td>
</tr>
<tr>
<td>CSCtz04599</td>
<td>MU: Cat4500: dot1x fail - MAB success - dot1x fail leads to High CPU</td>
</tr>
<tr>
<td>CSCty56801</td>
<td>NEAT: Bus error @ <code>__be_cisp_client_match</code> on Asw</td>
</tr>
<tr>
<td>CSCtw95189</td>
<td>DHCP error log - &quot;%Unknown DHCP problem.. No allocation possible&quot;</td>
</tr>
<tr>
<td>CSCty79277</td>
<td>Line protocol stays down after Authz success &amp; traffic is allowed</td>
</tr>
<tr>
<td>CSCtx53448</td>
<td>MA:Mab port interruption allows traffic to and fro unauthorized mab host</td>
</tr>
<tr>
<td>CSCtx64347</td>
<td>OpenAccess: Data mac blocked on interrupting authenticated port</td>
</tr>
<tr>
<td>CSCty25810</td>
<td>Tracebacks @ auth_feature_critical_get_authorized_domain_any</td>
</tr>
<tr>
<td>CSCej11786</td>
<td>Router reloads @ clear_dspm_counter_per_bay</td>
</tr>
<tr>
<td>CSCtx45373</td>
<td>&quot;%VRF specified does not match this router&quot; message seen during reload</td>
</tr>
<tr>
<td>CSCty02403</td>
<td>EIGRP topo entry with bogus nexthop created when SoO and TAG are present</td>
</tr>
<tr>
<td>CSCtx04709</td>
<td>Invalid entry stuck in EIGRP topology table until cleared manually</td>
</tr>
<tr>
<td>CSCtw61192</td>
<td>Routes are Stuck-In-Active state when routes are withdrawn from EIGRP</td>
</tr>
<tr>
<td>CSCty37445</td>
<td>Split Horizon Automatically turned off with distribute-list route-map</td>
</tr>
<tr>
<td>CSCty55449</td>
<td>Device crashes when EEM trigger is misconfigured</td>
</tr>
<tr>
<td>CSCtw86712</td>
<td>ASR1K: RP Crashes@oce_base_explore_chain</td>
</tr>
<tr>
<td>CSCtz03779</td>
<td>ASR903:Stdby crash @ fib_vrf_mgr_lookup_vrf on ISSU from 3.6 -&gt; 3.5</td>
</tr>
<tr>
<td>CSCtu22167</td>
<td>RP crash due to mistral error interrupt on LC OIR</td>
</tr>
<tr>
<td>CSCtw26683</td>
<td>RPF chk not supported on tunnel but getting configured.</td>
</tr>
<tr>
<td>CSCtu07968</td>
<td>ISR 890: Perf mon reports incorrect loss packets/percent with 0 loss</td>
</tr>
<tr>
<td>CSCtw61872</td>
<td>Possible crash from show flow monitor &lt;xxxx&gt; cache on multiple sessions</td>
</tr>
<tr>
<td>CSCts83046</td>
<td>ping fail as packet gets dropped in inband code due to IDB throttling</td>
</tr>
<tr>
<td>CSCtx31294</td>
<td>Ikey2 doesn't come up if headend Local auth is RSA-SIG, for AC clients</td>
</tr>
<tr>
<td>CSCtq84313</td>
<td>CPUHOG due to IP SLA followed by watchdog crash on replacing config</td>
</tr>
<tr>
<td>CSCty54446</td>
<td>CPU shoots up 99% all time, when WebAuth enabled and client request http</td>
</tr>
<tr>
<td>CSCtx56174</td>
<td>Router hang / crash with Websense URL Filtering or ZBFW HTTP ALG</td>
</tr>
<tr>
<td>CSCtq51039</td>
<td>Traffic being blocked with Waas + Ipsec + no policy on traffic</td>
</tr>
<tr>
<td>CSCty69981</td>
<td>Crash @: <code>__be_ips_port_map_scan</code></td>
</tr>
<tr>
<td>CSCtz27137</td>
<td>Installing S639 or later Signature Package Causes Crash Loop</td>
</tr>
<tr>
<td>CSCtz79991</td>
<td>Router crashes @ lic_install_notify_and_print_output</td>
</tr>
<tr>
<td>CSCtx96779</td>
<td>Crash at <code>__be_cont_scan_get_10_session</code> with simultaneous access</td>
</tr>
<tr>
<td>CSCtz34228</td>
<td>NTLM Passive Authentication Fails After Reload</td>
</tr>
<tr>
<td>CSCtz88595</td>
<td>NTLM VIP Popup shows as actual server URL instead of VIP address</td>
</tr>
<tr>
<td>CSCua22313</td>
<td>HTTPS page dont get displayed with IE6 conn optim by WAAS Express 2.0</td>
</tr>
<tr>
<td>CSCtx62920</td>
<td>One connection hang after sslao stress testing</td>
</tr>
<tr>
<td>CSCtz85134</td>
<td>WAAS Express SSL-Express changes self-signed trustpoint after reload</td>
</tr>
<tr>
<td>CSCty91465</td>
<td>Enabling CEF causing pings between VRF and global routing table to break</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCtz62766</td>
<td>Multiple LC crashes due to CEF LC Stats CPUHOG</td>
</tr>
<tr>
<td>CSCua43930</td>
<td>&quot;Checksum value parsed from GRE Header is incorrect&quot;</td>
</tr>
<tr>
<td>CSCts82058</td>
<td>Creation of Overlay interface leading (tunn) to continuous router crash</td>
</tr>
<tr>
<td>CSCts27333</td>
<td>MTU inconsistent in the standby VSS sup, traffic punted in some cases</td>
</tr>
<tr>
<td>CSCtz73157</td>
<td>cube send 0.0.0.0 when 9971 has video enabled for hold/resume</td>
</tr>
<tr>
<td>CSCty63868</td>
<td>Hard : CUBE crashed @:sipSPICheckHeaderSupport</td>
</tr>
<tr>
<td>CSCty43587</td>
<td>Router crash in SIP due to memory corruption</td>
</tr>
<tr>
<td>CSCtz33536</td>
<td>SIP KPML subscription fails after an expiration</td>
</tr>
<tr>
<td>CSCty53243</td>
<td>[XE3.7] Video Call is failing in the latest mcp_dev image - 20120303</td>
</tr>
<tr>
<td>CSCtt17762</td>
<td>mtrace output missing path information</td>
</tr>
<tr>
<td>CSCtx55357</td>
<td>multicast boundary doesn’t block Auto RP on ASR1k</td>
</tr>
<tr>
<td>CSCtx32329</td>
<td>V6Mcast : Switch crashes on shutting down an RPF intf of static mroute</td>
</tr>
<tr>
<td>CSCua35884</td>
<td>Issue with CLI ipv6 cef inside Serial/ATM interface in 3900 platform</td>
</tr>
<tr>
<td>CSCtr45287</td>
<td>3900 router crashes when the dvti tunnel count reaches 2500+</td>
</tr>
<tr>
<td>CSCtz78194</td>
<td>ASR 3.6 crash in IPSEC key engine w/large IKE profile names</td>
</tr>
<tr>
<td>CSCtr36083</td>
<td>ASR1000: clear crypto session local addr doesn’t clear IKE SA’s</td>
</tr>
<tr>
<td>CSCty52047</td>
<td>ASR1k - DPD not deleting IKE SA (release 3.5 and later)</td>
</tr>
<tr>
<td>CSCtw78451</td>
<td>ASR1k May reload when multiple users are issuing show commands</td>
</tr>
<tr>
<td>CSCts85459</td>
<td>C881GW : On Reload, cellular int won’t negotiate if crypto map applied</td>
</tr>
<tr>
<td>CSCua33821</td>
<td>crypto_acl: CPU utilization shoots up to 99% after config crypto maps</td>
</tr>
<tr>
<td>CSCtq39602</td>
<td>DMVPN Spoke stuck in IKE state after heavy traffic</td>
</tr>
<tr>
<td>CSCua78782</td>
<td>EzVPN Connection down due IPSEC SA nego failure on Inception</td>
</tr>
<tr>
<td>CSCtx44060</td>
<td>Flexvpn spoke to spoke tunnel doesn’t come up</td>
</tr>
<tr>
<td>CSCtx49766</td>
<td>GETVPN tracebacks with 3g/4g HWIC</td>
</tr>
<tr>
<td>CSCtz63438</td>
<td>GM continuously registers to KS after removing crypto engine accelerator</td>
</tr>
<tr>
<td>CSCtx93598</td>
<td>ikev1 dpd config erroneously affect ikev2 flows</td>
</tr>
<tr>
<td>CSCtw46061</td>
<td>Irremovable IPSec Sessions in &quot;show crypto eli&quot;</td>
</tr>
<tr>
<td>CSCty80553</td>
<td>Multicast over IPSEC crashes router</td>
</tr>
<tr>
<td>CSCtx04712</td>
<td>removing gdoi crypto-map from interface hangs the router</td>
</tr>
<tr>
<td>CSCua15292</td>
<td>router crashed at be_crypto_check_acl</td>
</tr>
<tr>
<td>CSCty61212</td>
<td>Router gets hanged while unconfiguring crypto map tag</td>
</tr>
<tr>
<td>CSCtz14980</td>
<td>stby RP keep reboot after SSO when configured crypto map GETVPN_MAP</td>
</tr>
<tr>
<td>CSCtw50952</td>
<td>ASR crashes due to memory exhaustion after issuing &quot;clear ip ospf&quot;</td>
</tr>
<tr>
<td>CSCtz72044</td>
<td>EzVPN client re-transmitting wrong packet=&gt; death by retransmission throw</td>
</tr>
<tr>
<td>CSCtz02622</td>
<td>FlexVPN spoke crashed while passing traffic</td>
</tr>
<tr>
<td>CSCtz47873</td>
<td>Flexvpn: &quot;sh crypto ikev2 client flex&quot; doesn't work as expected</td>
</tr>
<tr>
<td>CSCtx32527</td>
<td>Flexvpn: IPSEC SA on GRE tunnel should act as always-up like ipsec-ipv4</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCty84989</td>
<td>IKEv2+TP+VRF fails installing ipv6 ike routes in the ivrf</td>
</tr>
<tr>
<td>CSCtz40621</td>
<td>Crash observed when GM tries to register to KS and KS has issued rekey</td>
</tr>
<tr>
<td>CSCtz90154</td>
<td>GETVPN rapid re-registartion after ipsec failure during registration</td>
</tr>
<tr>
<td>CSCtv28434</td>
<td>GETVPN: tracebacks during GM re-registration</td>
</tr>
<tr>
<td>CSCtr93412</td>
<td>XE35 GETVPN - IGMP/PIM Crash Seen on Mwheel Process</td>
</tr>
<tr>
<td>CSCtx90408</td>
<td>Crash after configuring a crypto map on a HSRP enabled interface</td>
</tr>
<tr>
<td>CSCtx50176</td>
<td>ASR1k :ikev2 brings up sa even with CRYPTO_ERR_RESOURCES from dh</td>
</tr>
<tr>
<td>CSCtx31329</td>
<td>Memory leak in ikev2_process_config_setAttribs</td>
</tr>
<tr>
<td>CSCtt70133</td>
<td>RP crash @ __be_ikey2_bin2hex_str due to crypto_engine: no resources err</td>
</tr>
<tr>
<td>CSCtw79510</td>
<td>Cant force VPN client users to change their passwords in the nxt login</td>
</tr>
<tr>
<td>CSCtx73612</td>
<td>ASR crash while performing SNMP of IPsec stats.</td>
</tr>
<tr>
<td>CSCtx23534</td>
<td>RRI Host Routes not replicated to HA peer</td>
</tr>
<tr>
<td>CSCtw98456</td>
<td>Static and dynamic RRI create incorrect route in vrf-aware IPSec case</td>
</tr>
<tr>
<td>CSCtx90293</td>
<td>GREv6 over IPv6 improvements</td>
</tr>
<tr>
<td>CSCtz08037</td>
<td>OCE Handle Leak with dual tunnel encryption</td>
</tr>
<tr>
<td>CSCtx92802</td>
<td>Packet drops with VFR and crypto tunnel</td>
</tr>
<tr>
<td>CSCtt45654</td>
<td>Virtual-Access is not deleted when tear down ipsec session</td>
</tr>
<tr>
<td>CSCtx07394</td>
<td>887VA ADSL LFI PPPOA router cannot pass packets larger than 1494 bytes</td>
</tr>
<tr>
<td>CSCty03629</td>
<td>ISR-CTS : Security Group aware Firewall does not work with NAT</td>
</tr>
<tr>
<td>CSCtu16862</td>
<td>L4F tracebacks observed with SMB stress test traffic.</td>
</tr>
<tr>
<td>CSCtx40818</td>
<td>Session failure in VPN+FW+NAT+QOS test: %IP-3-LOOPPAK and %FW-6-DROP_PKT</td>
</tr>
<tr>
<td>CSCtx06801</td>
<td>SS: Certain websites may load slowly</td>
</tr>
<tr>
<td>CSCty85634</td>
<td>LISP map cache entries lost after RP switch when VRFs configured</td>
</tr>
<tr>
<td>CSCty46273</td>
<td>LISP route watch notification may end up dereferencing NULL route</td>
</tr>
<tr>
<td>CSCtx38674</td>
<td>UUT can not establish a call using Dialer with no ip address</td>
</tr>
<tr>
<td>CSCty17288</td>
<td>OIDs looping infinitely with media-mon cfg and traffic</td>
</tr>
<tr>
<td>CSCtx48753</td>
<td>ASR1K: 10% Increase in IOS Mem in BBA Profiles in XE36</td>
</tr>
<tr>
<td>CSCtx57073</td>
<td>ISSU:XE3.6---&gt;MCP_DEV iosd crash @ Process = Metadata HA</td>
</tr>
<tr>
<td>CSCua60785</td>
<td>Metadata class-map matches only the first match statement for mediatype</td>
</tr>
<tr>
<td>CSCtw73530</td>
<td>Metadata: flow gen fail to clear created flows with 100 or more flows</td>
</tr>
<tr>
<td>CSCtz59429</td>
<td>MF: metadata not matching &quot;application attribute category voice-video&quot;</td>
</tr>
<tr>
<td>CSCtz24280</td>
<td>MSP does not recognize Polycom flows because of Proxy-address field</td>
</tr>
<tr>
<td>CSCty13747</td>
<td>nbar applications with engine-id=13 not shown/exported by flow exporter</td>
</tr>
<tr>
<td>CSCtx92665</td>
<td>Crash at __be_sla_mt_route_data_print with show cmd after link flap</td>
</tr>
<tr>
<td>CSCtx87939</td>
<td>XML output for mediatrace poll command is invalid</td>
</tr>
<tr>
<td>CSCtz00431</td>
<td>EPC_ASR1k: Crash on restarting cap point after removing associated policy</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSCty41067</td>
<td>Router crashes while doing SSO in latest rls10 image</td>
</tr>
<tr>
<td>CSCty12524</td>
<td>BRA from MAG is missing Service Selection having APN &amp; HOA options</td>
</tr>
<tr>
<td>CSCtx52042</td>
<td>LMA/MAG crash when clear bindings for the peer.</td>
</tr>
<tr>
<td>CScua06629</td>
<td>sh ipv6 mobile pmpipv6 mag globals command is broken</td>
</tr>
<tr>
<td>CSCua18138</td>
<td>If enable mobile ip function, c819 crashed after cable removed</td>
</tr>
<tr>
<td>CSCtx67290</td>
<td>[XE36] sbc crash when receive anomaly rtcp-fb element in SDP</td>
</tr>
<tr>
<td>CSCty26126</td>
<td>plain IP packets should not have a label</td>
</tr>
<tr>
<td>CSCty71843</td>
<td>Traceback @ lfd_sm_start/lfd_sm_handle_event_state_stopped during bootup</td>
</tr>
<tr>
<td>CSCua33527</td>
<td>:%LFD-SW2-3-SMBADEVENT:TRACEBACK seen after 2nd &amp; 3rd switch over</td>
</tr>
<tr>
<td>CSCtx25953</td>
<td>LFD-3-CORRUPTED_PKT: exception packet with NULL inlabel pointer</td>
</tr>
<tr>
<td>CSCtx06813</td>
<td>lfd_install_local_label_for_key: installation failed for rwid type l2ckt</td>
</tr>
<tr>
<td>CSCtx34643</td>
<td>ping MPLS Psedowire is not working with single segment</td>
</tr>
<tr>
<td>CSCtz41048</td>
<td>trace mpls ipv4 is unsuccessful in latest PI19</td>
</tr>
<tr>
<td>CSCtr25127</td>
<td>Traceback observed with switching between ATM and 3G interface</td>
</tr>
<tr>
<td>CSCtt04093</td>
<td>VC is not coming up after unshutting the preferred path/Tunnel</td>
</tr>
<tr>
<td>CSCtu35116</td>
<td>VPDN sessions doesn't come up with &quot;mpls mtu&quot; more than 1500 byte</td>
</tr>
<tr>
<td>CSCty54728</td>
<td>MF: media-proxy services metadata/rsvp parser inconsistency</td>
</tr>
<tr>
<td>CSCtz73263</td>
<td>MSP: MSP not working on ISR SVI interfaces</td>
</tr>
<tr>
<td>CSCty97784</td>
<td>Crash in NBAR at action_flowvar_operator</td>
</tr>
<tr>
<td>CSCty48870</td>
<td>NBAR crash at action_add_standard_global with reassembled packet</td>
</tr>
<tr>
<td>CSCtz94964</td>
<td>Nbar fails to recognize traffic in the match protocol http url/host</td>
</tr>
<tr>
<td>CSCtd67668</td>
<td>crash with netflow on virtual-template</td>
</tr>
<tr>
<td>CSCua31934</td>
<td>Crash seen at __be_address_is_unspecified</td>
</tr>
<tr>
<td>CSCty90223</td>
<td>Crash seen at nhrp_nhs_recovery_co_destroy during setup and config</td>
</tr>
<tr>
<td>CSCtx52095</td>
<td>I/O Leak for Middle Buffer at nhrp_getbuffer</td>
</tr>
<tr>
<td>CSCtz76650</td>
<td>IPv6 nhrp phase 2 doesn't work with EIGRP or OSPF as routing protocol</td>
</tr>
<tr>
<td>CSCty22840</td>
<td>Router crashes due to CPU Watchdog on NTP Process</td>
</tr>
<tr>
<td>CSCtv36812</td>
<td>MF: IOSd log displays incorrect crashinfo filename</td>
</tr>
<tr>
<td>CSCtu40028</td>
<td>Scheduler process reload on ASR1000 ASR903</td>
</tr>
<tr>
<td>CSCty76106</td>
<td>Whales1 crashed after more than 2 days of soak with traffic</td>
</tr>
<tr>
<td>CSCts44393</td>
<td>ASR crashed at reg_inv_find_path under BGP stress test</td>
</tr>
<tr>
<td>CSCtx57784</td>
<td>NG3K: Configuring 'logging persistent url' command crashes the device</td>
</tr>
<tr>
<td>CSCty05150</td>
<td>OSPF default summary route withdrawn after SSO switchover on ABR</td>
</tr>
<tr>
<td>CSCty68348</td>
<td>ospf state not synced to stdby after shut/no shut of ospf proc on active</td>
</tr>
<tr>
<td>CSCtx74342</td>
<td>ospfv3 route to connected prefix points to down interface until next spf</td>
</tr>
<tr>
<td>CSCty08070</td>
<td>OSPFv3: Traceback@process_events_waiting_p</td>
</tr>
<tr>
<td>CSCua29428</td>
<td>Add rip routing support for vg350</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCtu23195</td>
<td>SNMP ifIndex for serial interfaces becomes inactive after PA OIR</td>
</tr>
<tr>
<td>CSCty01237</td>
<td>Crash related to prefix-list update</td>
</tr>
<tr>
<td>CSCty37020</td>
<td>Inside BGP learned prefixes not added to MC db</td>
</tr>
<tr>
<td>CSCtx35064</td>
<td>PFR - MC not declaring OOP for unreachable until Holddown timer expires</td>
</tr>
<tr>
<td>CSCts65564</td>
<td>DMVPN hub router crash when crl caching is disabled</td>
</tr>
<tr>
<td>CSCty32463</td>
<td>Kingpin &amp; 1RU Unable to sync in SSO mode w/ 'crypto pki' configuration.</td>
</tr>
<tr>
<td>CSCty51453</td>
<td>OCSP Bad requests - incorrect length or truncated payload</td>
</tr>
<tr>
<td>CSCty30886</td>
<td>Bringup PPPoE sessions with invalid IP local pool crashes standby RP.</td>
</tr>
<tr>
<td>CSCtw46229</td>
<td>PPP LCP ConfReq Small buffer leak</td>
</tr>
<tr>
<td>CSCtx66804</td>
<td>ppp lcp delay 0 does not work</td>
</tr>
<tr>
<td>CSCts68626</td>
<td>PPPoE discovery packets causes packet drop</td>
</tr>
<tr>
<td>CSCty32851</td>
<td>Router may crash when changing encap type on serial interface to mlpppp</td>
</tr>
<tr>
<td>CSCtx37863</td>
<td>Upon IPCP negotiation failure, BRAS should send Interim + free ipv4 addr.</td>
</tr>
<tr>
<td>CSCty94289</td>
<td>Flexwan - Drop Rate is nearly 1mbps with priority configuration</td>
</tr>
<tr>
<td>CSCty68402</td>
<td>mod4 account is not working</td>
</tr>
<tr>
<td>CSCtu14409</td>
<td>Not able to update a policy with priority to pri + police</td>
</tr>
<tr>
<td>CSCtz86747</td>
<td>Router crashes upon removing all the class-map from policy-map</td>
</tr>
<tr>
<td>CSCtu43120</td>
<td>Service Accounting START not sent for L2TP sessions</td>
</tr>
<tr>
<td>CSCtw62310</td>
<td>xe36:rem pmap from int changes the random-detect dscp attr with &quot;cells&quot;</td>
</tr>
<tr>
<td>CSCty98365</td>
<td>mcp_dev crashes in rf mib code for b2b</td>
</tr>
<tr>
<td>CSCtu32301</td>
<td>I/O Memory fragmentation on executing show tech command at linecard</td>
</tr>
<tr>
<td>CSCty49656</td>
<td>Crash @ ip_route_delete_common when &quot;no ip routing&quot; is issued on console</td>
</tr>
<tr>
<td>CSCty05092</td>
<td>Eigrp doesn't remove connected route from topology after int shutdown</td>
</tr>
<tr>
<td>CSCtx45970</td>
<td>Crash with group scheduling when freq. is not multiple of history interv</td>
</tr>
<tr>
<td>CSCty23094</td>
<td>Router reboots @ 0x766F6E4:slaRespPerformRoutineChecks during traffic</td>
</tr>
<tr>
<td>CSCua64100</td>
<td>Issue in SCTP Receive message</td>
</tr>
<tr>
<td>CSCty04384</td>
<td>IMA-DSLAPP Crash with ASAM 7300 -SMLT-C and Lucent Stinger</td>
</tr>
<tr>
<td>CSCua84879</td>
<td>Crash at slaVideoOperationPrint_ios with show running-config</td>
</tr>
<tr>
<td>CSCtz67726</td>
<td>IP SLA - ip sla group schedule issue with single SLA probe ID</td>
</tr>
<tr>
<td>CSCua19294</td>
<td>IP SLA udp-jitter operation intermittently report wrong minimum RTT</td>
</tr>
<tr>
<td>CSCtz97244</td>
<td>IP SLA video operation fails in a VRF with “Timeout” as return code</td>
</tr>
<tr>
<td>CSCua45548</td>
<td>Router crashes with &quot;sh ip sla summary&quot; on longevity testing</td>
</tr>
<tr>
<td>CSCjt95182</td>
<td>High CPU on 3750 when network scanner is run</td>
</tr>
<tr>
<td>CSCty32232</td>
<td>BRI interfaces are shown as unmonitored till reload.</td>
</tr>
<tr>
<td>CSCtt20719</td>
<td>Incremental leaks at shdsl_efmEndpointCurrEntry_get and other funcs</td>
</tr>
<tr>
<td>CSCty29122</td>
<td>Tcp tls handshake fails for Secure RTP calls (unset SO_NBIO option fail)</td>
</tr>
<tr>
<td>CSCtd86428</td>
<td>ssh session not accept IPv6 addr in VRF Interface, but accepts IPv4 addr</td>
</tr>
<tr>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCtw55424</td>
<td>SSH support for vrf with ipv6 addr/hostname</td>
</tr>
<tr>
<td>CSCty77190</td>
<td>DTLS based SSLVPN tunnel fails in case of vrf and session reconnect</td>
</tr>
<tr>
<td>CSCsw95673</td>
<td>ENH: Support for OTP with RADIUS Access-Challenge message in IOS SSL VPN</td>
</tr>
<tr>
<td>CSCts32708</td>
<td>IOS SSLVPN stops accepting new SSL connections, stuck TCP CLOSED conns</td>
</tr>
<tr>
<td>CSCtw58664</td>
<td>SSL VPN for SCCP causes crash while clearing WebVPN session</td>
</tr>
<tr>
<td>CSCty92182</td>
<td>stack overflow for &quot;cifs_browse_share_sync function&quot;</td>
</tr>
<tr>
<td>CSCtz96167</td>
<td>QoS signaling marking dscp 31 not working</td>
</tr>
<tr>
<td>CSCty80566</td>
<td>UC560 15.1(4)M2 crash</td>
</tr>
<tr>
<td>CSCtz02182</td>
<td>FlexVPN: tracebacks were seen while adding int virtual-template type</td>
</tr>
<tr>
<td>CSCzw78868</td>
<td>sp2600(pvdm3) 2.24 fax library commit</td>
</tr>
<tr>
<td>CSCtx77750</td>
<td>Crosstalk may be heard by PSTN callers during call on hold (MMoH)</td>
</tr>
<tr>
<td>CSCtx28483</td>
<td>ASR1k:CUBE: Redundancy reboot during configuration change</td>
</tr>
<tr>
<td>CSCty24606</td>
<td>ASR1k:CUBE: Hung call legs after failover not deleted by media inactivity</td>
</tr>
<tr>
<td>CSCtx90703</td>
<td>CM tone squelched during protocol based modem pass through</td>
</tr>
<tr>
<td>CSCtx54882</td>
<td>Router may crash due to bus error - voip_rtp_dispose_media_service_pak</td>
</tr>
<tr>
<td>CSCty83520</td>
<td>RTCP packet sent to Multicast MoH IP address by H.323 TDM Gateway</td>
</tr>
<tr>
<td>CSCty04798</td>
<td>Memory leak in show_voice_call_status_task</td>
</tr>
<tr>
<td>CSCtx57584</td>
<td>SIP basic call fails with 500 Internal server error</td>
</tr>
<tr>
<td>CSCtt26692</td>
<td>chunk corruption due to sipSPITranslateOutRedirectCalled.</td>
</tr>
<tr>
<td>CSCtx66030</td>
<td>Crash in sipSPI_ipip_AddPassthruHdhrsToMsgContainer</td>
</tr>
<tr>
<td>CSCtx95840</td>
<td>Crash on voice gateway in cnfsm_exec()</td>
</tr>
<tr>
<td>CSCty61216</td>
<td>Memory leak in CCSIP_SPI_CONTROL</td>
</tr>
<tr>
<td>CSCtt26208</td>
<td>Memory Leak in CCSIP_SPI_CONTROL @ cc_api_get_call_active_entry</td>
</tr>
<tr>
<td>CSCtx86539</td>
<td>NAT SIP ALG changes Media Attributes</td>
</tr>
<tr>
<td>CSCtx79318</td>
<td>OGW Failed to send 200 OK response for OPTION</td>
</tr>
<tr>
<td>CSCty58992</td>
<td>One way audio with SIP POTS phone</td>
</tr>
<tr>
<td>CSCtx84059</td>
<td>SIP-One-way audio on SIP CFU calls and GW uses route map.</td>
</tr>
<tr>
<td>CSCtt21456</td>
<td>Unexpected reload due to CCSIP_SPI_CONTROL process</td>
</tr>
<tr>
<td>CSCtz99916</td>
<td>3945 is not responding to reinvite from CVP</td>
</tr>
<tr>
<td>CSCty41850</td>
<td>MGCP GW with PVDM3 advertises G723 which it can't support</td>
</tr>
<tr>
<td>CSCtz22112</td>
<td>VXML gateway crash when trying to access a URL.</td>
</tr>
<tr>
<td>CSCtz45901</td>
<td>show run</td>
</tr>
<tr>
<td>CSCty12083</td>
<td>C819HG+7 platform getting reloads</td>
</tr>
<tr>
<td>CSCtz33622</td>
<td>Multiple crashes on ISR routers due to a managed timer corruption</td>
</tr>
<tr>
<td>CSCsts56278</td>
<td>2951, 3925, 3945 Systems IOS Machine Check with SM in Slot 1</td>
</tr>
</tbody>
</table>
Bugs for Cisco IOS Release 15.2(3)T

Bugs

Bugs describe unexpected behavior in Cisco IOS software releases. Severity 1 bugs are the most serious bugs; severity 2 bugs are less serious. Severity 3 bugs are moderate bugs, and only select severity 3 bugs are included in this section.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select bugs of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

- Resolved Bugs—Cisco IOS Release 15.2(3)T4, page 272
- Resolved Bugs—Cisco IOS Release 15.2(3)T3, page 277
- Resolved Bugs—Cisco IOS Release 15.2(3)T2, page 294
- Resolved Bugs—Cisco IOS Release 15.2(3)T1, page 310
- Open Bugs—Cisco IOS Release 15.2(3)T, page 329
- Resolved Bugs—Cisco IOS Release 15.2(3)T, page 330
Resolved Bugs—Cisco IOS Release 15.2(3)T

- CSCsq83006
  Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.
  Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which are connected via a partial mesh port-channel.
  Workaround: Use the port-channel interface settings below:

  ```
  (config)# interface port-channel <port-channel interface number>
  (config-if)# bandwidth <bandwidth value>
  (config-if)# delay <delay value>
  ```

  Further Problem Description: If a test is done with a physical interface, not a port-channel, this issue is not seen.

- CSCts55778
  Symptoms: This is a problem involving two SAF forwarders, where one is running EIGRP rel8/Service-Routing rel1 and the other is running EIGRP dev9/Service-Routing dev2. The capabilities-manager, a client of the service-routing infrastructure, will advertise two services. When forwarders are peering with the same release image, the services propagate between the forwarders without any problems. But, when you run rel8/rel1 on one forwarder, and dev9/dev2 on the other forwarder, a third service appears in the topology table and the SR database that was not advertised.
  Note: The problem cannot be recreated if both forwarders are running an Cisco IOS XE Release 3.4S or and Cisco IOS XE Release 3.5S image.
  Conditions: This symptom occurs if two SAF forwarders peer with each other, where one SAF forwarder is running EIGRP SAF release 9 or above and the other SAF forwarder is running EIGRP SAF release 8 or below.
  Workaround: Make sure each SAF forwarder is running EIGRP release 8 or below, or release 9 or above.

- CSCtw78539
  Symptoms: A Cisco ISR router running Cisco IOS Release 15.2(2)T may lose the ability to forward traffic via its Gigabit Ethernet interface due to a stuck Tx ring.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T1, 15.2(2)T, and 15.2(4)M. This is a regression issue that does not affect 15.0(1)M3 nor 15.1(4)M2 based on anecdotal accounts.
  During the event the following logs can be seen which indicate a spurious memory access has occurred:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0xXXXXXXXX reading 0x0
  %ALIGN-3-TRACE: -Traceback= 0xXXXXXXXX ...
  ```

  At this time, the Tx ring of the interface becomes hung, causing packet drops to accumulate at the output queue (as seen via “show interface”), effectively preventing traffic flow. For Example:

  ```
  Total output drops: 25185 Output queue: 331/1000/25184 (size/max total/drops)
  ```

  Workaround: Reload the router or bounce the interface via “shut/no shut”.

---

Bugs for Cisco IOS Release 15.2(3)T

OL-25471-04 Rev. P0
• **CSCtx56174**
  Symptoms: Cisco router hangs until a manual power cycle is done. If the `scheduler isr-watchdog` command is configured, the device will crash and recover instead of hanging until a power cycle is done.
  Conditions: This is seen with websense URL filtering enabled and with zone based firewalls.
  Workaround: Disable URL-based filtering.

• **CSCty96049**
  Summary: Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.
  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:
  Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2012 bundled publication.
  Individual publication links are in “Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication” at the following link:
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.8/6.4:
  CVE ID CVE-2012-4621 has been assigned to document this issue.
  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

• **CSCud41058**
  Symptoms: There is a route-map which matches tags and set a new value. This route-map is used in an EIGRP outbound distribute list. One in 10 times based on the received route tag, the correct route tag value is not set while advertising out.
  Conditions: The symptom is observed when you use a route map which matches tags and sets a new tag. Used in `distribute-list route-map name out`.
  Workaround: Clear the EIGRP process or re-advertise the route.

• **CSCud55286**
  Symptoms: Traffic drops for sometime after doing a switchover.
  Conditions: The symptom is observed when a switchover is performed on a Cisco ASR 903.
  Workaround: Put a neighbor command where the neighbor has no meaning and will never be up. This will solve the timing issue.

• **CSCud79067**
  Symptoms: The BGP MIB reply to a getmany query is not lexicographically sorted.
Conditions: This symptom is observed when IPv4 and IPv6 neighbor IP addresses are lexicographically intermingled, for example, 1.1.1.1, 0202::02, 3.3.3.3.

Workaround: There is no workaround.

- **CSCue26213**
  
  Symptoms: The connected interface that is enabled for EIGRP will not be redistributed into BGP.
  
  Conditions: This symptom occurs when the prefix of the connected interface is in the EIGRP topology table with “redistribute eigrp” under BGP address-family IPv4.
  
  Workaround: Redistribute the connected interface and EIGRP.

- **CSCue36197**
  
  Symptoms: The Cisco 7600 router may crash while performing the NSF IETF helper function for a neighbor over a sham-link undergoing NSF restart.
  
  Conditions: This symptom occurs when a router is configured as an MPLS VPN PE router with OSPF as PE-CE protocol. OSPF in VRF is configured with a sham-link and a neighbor router over a sham-link is capable of performing an NSF IETF restart on sham-links.
  
  Note: This problem cannot be seen if both routers on sham-link ends are Cisco IOS routers.
  
  Workaround: Disable the IETF Helper Mode protocol by entering the following commands:

  ```
  enable configure terminal router ospf process-id [vrf vpn-name] nsf ietf helper disable end
  ```
  
  Note: Disabling Helper Mode will result in an OSPF peer dropping adjacency if the peer is reloaded.

- **CSCue69214**
  
  Symptom: Memory leaks are seen in the metadata after removing a virtual interface.
  
  Conditions: This symptom occurs after removing a virtual interface, if metadata is enabled.
  
  Workaround: There is no workaround.

- **CSCue94880**
  
  Symptoms: RTP traffic fails in reverse direction when an outside source list is configured and RTP SA IP matches against this list.
  
  Conditions: The symptom is observed with a Cisco IOS version above 12.4(9) mainline.
  
  Workaround: Use Cisco IOS Release 12.4(9).

- **CSCuf09006**
  
  Symptoms: Upon doing a `clear ip bgp * soft out` or `graceful shutdown` on a PE, all VPNv4/v6 routes on an RR from this PE are purged at the expiry of enhanced refresh stale-path timer.
  
  Conditions: The symptom is observed with the following conditions:

  1. PE must have BGP peering with at least one CE (VRF neighbor) and at least one RR (VPN neighbor).
  2. PE must have a rtfilter unicast BGP peering with the RR.
  3. IOS version must have “Enhanced Refresh” feature enabled.
  4. A `clear ip bgp * soft out` or `graceful shutdown` is executed on the PE.
  
  Workaround: Instead of doing `clear ip bgp * soft out`, do a route refresh individually towards all neighbors.

- **CSCuf17023**
Symptom: A vulnerability in the Resource Reservation Protocol (RSVP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger an interface queue wedge on the affected device.

The vulnerability is due to improper parsing of UDP RSVP packets. An attacker could exploit this vulnerability by sending UDP port 1698 RSVP packets to the vulnerable device. An exploit could cause Cisco IOS Software and Cisco IOS XE Software to incorrectly process incoming packets, resulting in an interface queue wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-rsvp

Symptom: The Cisco IOS Software implementation of the network address translation (NAT) feature contains three vulnerabilities when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are not available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-nat

Conditions: See advisory for details

Workaround: There is no workaround.

Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication. Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

Symptom: In certain scenarios, EIGRP routes are advertised only to Stub peers, not advertised to Non-Stub Peers.

EIGRP Routes - Routes in EIGRP Topo table. It can be routes learnt by EIGRP peer OR redistributed also.

Conditions: This symptom is observed when Cisco ASR router is rebooted or the route is cleared via the `clear ip route` command, the route disappears form the spokes. This bug is not restricted to ASR. It can happen with any kind of router with following conditions met.

1. Peers to be mixture of Stubs and Non Stubs.
2. When Route is Lost, we send QUERY to non-stubs and waiting for REPLY from Non Stubs about QUERY.
3. A new update needs to be sent to all Peers.
Bugs for Cisco IOS Release 15.2(3)T

Workaround: Advised to upgrade to image with Fix. Clearing the EIGRP Neighborship restores the route on the spokes.

More Information: To explain, in an ideal scenario, sequence is:

1. When route is lost, send QUERY to Non-Stubs.
2. After receiving REPLY from Non-Stubs, send infinite metric to Stub peers.
3. Route learnt again.
4. Route advertised to both Stub and Non-Stub peers properly.

In a defect scenario, (for example clear route), as new route is learnt before getting REPLY from Non-Stubs especially when Non-Stub neighbors/networks beyond Non-Stubs are more sequential “c” comes before “b”. In such cases routes were sent only to Stub.

- CSCug31561

A vulnerability in the DHCP implementation of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability occurs during the parsing of crafted DHCP packets. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that has the DHCP server or DHCP relay feature enabled. An exploit could allow the attacker to cause a reload of an affected device.

Cisco has released free software updates that address this vulnerability. There are no workarounds to this vulnerability.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp

Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- CSCug34485

Summary: Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

The attacker could trigger this vulnerability by injecting crafted OSPF packets. Successful exploitation could cause flushing of the routing table on a targeted router, as well as propagation of the crafted OSPF LSA type 1 update throughout the OSPF AS domain.

To exploit this vulnerability, an attacker must accurately determine certain parameters within the LSA database on the target router. This vulnerability can only be triggered by sending crafted unicast or multicast LSA type 1 packets. No other LSA type packets can trigger this vulnerability.

OSPFv3 is not affected by this vulnerability. Fabric Shortest Path First (FSPF) protocol is not affected by this vulnerability.

Workaround: Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.8/5.8:


CVE ID CVE-2013-0149 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:


- CSCug58383
  Symptom: Crash with %SYS-2-FREEFREE: Attempted to free unassigned memory at xxxxxxx (CSCue66692). Throttle breakage due to incompatible pointer assignment to data_to_block();
  Conditions: This symptom is observed when Cisco IOS is running on the router.
  Workaround: There is no workaround.

- CSCug72891
  Symptom: EIGRP neighbor flaps due to EIGRP SIA. Troubleshooting shows that a race condition causes EIGRP successor loop first and it leads to EIGRP QUERY loop resulting in the neighbor flaps.
  Conditions: The issue is observed when a worse metric update is received from the successor, once the route is already in active state, in a partially peered multiaccess network.
  Workaround: There is no workaround.

**Resolved Bugs—Cisco IOS Release 15.2(3)T3**

Cisco IOS Release 15.2(3)T3 is a rebuild release for Cisco IOS Release 15.2(3)T. The bugs in this section are resolved in Cisco IOS Release 15.2(3)T3 but may be open in previous Cisco IOS releases.

- CSCsy93069
  Symptoms: After a period of telepresence calls, tracebacks and then a router crash is seen.
  Conditions: The symptom is observed only when running Cisco IOS firewall with 17 SIP inspect policies applied. This crash happens at low scale with one CTS 3k call cycling with a hold time of 600 secs.
  It occurs intermittently and over time in an environment where there may be some call failures.
  Workaround: There is no workaround.

- CSCtj59117
  Symptoms: The following error message is seen and the router freezes and crashes:

  %SYS-2-BADSHARE: Bad refcount in retparticle
  A reload is required to recover.

  Conditions: The symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Release 12.4(15)T14.
  Workaround: Remove CEF.

- CSCtj95182
  Symptoms: Scanning for security vulnerabilities may cause High CPU condition on Cisco Catalyst 3750.
Conditions: Network scanner run against a 3750 running 12.2.55.SE.
Workaround: There is no workaround.

Additional Information: Vulnerable versions: 12.2(52)EX through 12.2(55)SE4, 15.1(3)T through 15.1(4)XB8a, 15.2(1)GC - 15.2(3)XA.
First fixed in: 12.2(55)SE5, 15.0(1)EX, 15.1(1)SG, 15.2(1)E, 15.2(4)M, 15.3(1)T.

In the meantime, Cisco has published several security advisories for Smart Install vulnerabilities:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smart-install

- CSCtq39602
Symptoms: DMVPN Tunnel is down with IPSEC configured. The `show dmvpn` from Spoke shows the state is IKE.
Conditions: After heavy traffic was pumping from DMVPN Hub to Spoke for some time, from a few minutes to a couple of hours.
Workaround: Configure "set security-association lifetime kilobytes disable" to disable volume based rekeying will reduce the problem.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6:
CVE ID CVE-2012-3915 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

- CSCts37446
Symptoms: Traceback is observed while testing the antireplay feature.
Conditions: Traceback is observed while configuring the routers randomly. It is not observed manually.
Workaround: There is no workaround.

- CSCts44393
Symptoms: A Cisco ASR 1000 crashes.
Conditions: The symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.
Workaround: There is no workaround.

- CSCtt45654
Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.
Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.
Workaround: There is no workaround.

- CSCtt70133
Symptoms: The RP resets with FlexVPN configuration.
Conditions: This symptom is observed when using the `clear crypto session` command on the console.
Workarounds: There is no workaround.

- CSCtu08373
Symptoms: Router crashes at various decodes including `fw_dp_base_process_pregen` and `cce_add_super_7_tuple_db_entry_common`.
Conditions: IOS firewall is configured and traffic is flowing through the router.
Workarounds: There is no workaround.

- CSCtu28696
Symptoms: A Cisco ASR 1000 crashes with `clear ip route`.
Conditions: The symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, then clear the configuration.
Workarounds: There is no workaround.

- CSCtu32301
Symptoms: Memory leak may be seen.
Conditions: This is seen when running large `show` commands like `show tech-support` on the linecard via the RP console.
Workarounds: Do not run the show commands frequently.

- CSCtu40028
Symptoms: The SCHED process crashes.
Conditions: The issue occurs after initiating TFTP copy.
Workarounds: There is no workaround.

- CSCtw46061
Symptoms: The following output shows the leaked SA object continuing to be in the “OBJECT_IN_USE” state. The state is supposed to be changed to OBJECT_FREEING by `crypto_engine_delete_ipsec_sa()`.
Conditions: This symptom is observed on a Cisco ASR 1000 series router.
Workarounds: There is no workaround.

- CSCtw78451
Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.
Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.
Bugs for Cisco IOS Release 15.2(3)T

Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw98456
Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

For example, the IVRF routing table should show:

```
S 10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
```

but instead it shows:

```
S 10.0.0.0 [1/0] via 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in `show crypto ipsec sa`) remain at zero.

Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

Workaround: Configure a static route to the remote network. For example:

```
ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtx04712
Symptoms: Removal of crypto map hangs the router.

Conditions: The symptom is observed following removal of “gdoi crypto map” from interface.

Workaround: There is no workaround.

- CSCtx31177
Symptoms: RP crash is observed on avl_search in a high scaled scenario.

Conditions: This symptom is observed in a high scaled scenario with continuous traffic flow.

Workaround: There is no workaround.

- CSCtx41296
Symptoms: When you do a clear crypto session in 4k flexVPN cases, the memory of crypto IKEv2 shows that it is increasing.

Conditions: The symptom is observed with session flapping.

Workaround: There is no workaround.

- CSCtx44060
Symptoms: Flexvpn spoke-to-spoke tunnels do not come up.

Conditions: None.

Workaround: Once tunnels fail to come up, clear the NHRP cache on one spoke alone.

- CSCtx50176
Symptoms: RP crashes @ be_ikev2_abort_negotiation.
Conditions: The symptom is observed while bringing up 4K SVTI_BGP with ike_group 16.
Workaround: There is no workaround.

- CSCtx57784
  Symptoms: Device crashes while configuring “logging persistent url”.
  Conditions: Occurs when the destination file system has zero free bytes left.
  Workaround: There is no workaround.

- CSCtx66011
  A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.
  The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).
  Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.
  In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.
  Only IKEv1 is affected by this vulnerability.
  An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.
  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.
  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ike
  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.
  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- CSCtx61815
  Symptoms: IPsec sessions are not coming up.
  Conditions: The symptom is observed when 1000 sessions are configured. Only 50 IPsec sessions are coming up.
  Workaroud: There is no workaround.

- CSCtx73612
  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.
Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

Workaround: Do not poll or trap IPsec information via SNMP.

- CSCtx90299
  Symptoms: The DMVPN IPsec sessions might get torn down and unable to re-establish themselves after experiencing link-flap events.
  Conditions: In a scaled DMVPN environment, when physical-port link-state up/down events happen, there will be stormed IPSec events to tear down and/or re-negotiate the sessions; it might run into a bad state that it cannot establish new sessions. Hence, when those active sessions expire (by time period or volume based), it can no longer be re-created. After some period of time, no more active session remains on the router.
  Workaround: Reload the router.

- CSCtx93598
  Symptoms: An “ikev1 dpd” configuration erroneously affects IKEv2 flows.
  Conditions: The symptom is observed if we configured the IKEv1 DPD function with “crypto isakmp keepalive” while IKEv2 is enabled as well. The IKEv2 DPD function will be affected.
  Workaround: There is no workaround.

- CSCty12055
  Symptoms: A Cisco ASR 1000 6RU acting as IPsec-DMVPN hub with 4K sessions up on the router may unexpectedly reload at “IPSec background proc” within a few hours.
  Conditions: The symptom is observed on a Cisco ASR 1000 6RU acting as IPsec-DMVPN hub.
  Workaround: There is no workaround.

- CSCty52047
  Symptoms: IKE SAs are not getting deleted by DPD (crypto isakmp keepalive).
  Conditions: This symptom is observed on a Cisco ASR 1000 router with DPD enabled.
  Workaround: Manually delete the stuck isakmp session:
  clear crypto isakmp conn-id
  You can get the conn-id from the output of the show crypto isakmp sa command.

- CSCty61212
  Symptoms: The removal of crypto map hangs the router.
  Conditions: This symptom is observed with the removal of GDOI crypto map from interface.
  Workaround: There is no workaround.

- CSCty79277
  Symptoms: Line protocol stays down after Authz success and traffic is allowed.
  Conditions: The symptom is observed with Cisco IOS Release 15.2(2)T, running on a Cisco 1900 platform, doing default inter Fa0/1/0 with 802.1x configurations and re-applying will authenticate the connected MAB supplicant. However, the interface’s line protocol remains in DOWN state and traffic will be allowed.
  Workaround: Do a shut and no shut and authenticate the connected supplicant.

- CSCty82414
Symptoms: Frequent crashes are seen with IPS enabled Firewall and passing TCP traffic. Trace decode points to the “ips_dp_feature_action_internal” function or nearby areas.
Conditions: This symptom occurs when IPS is enabled with Firewall in the router.
Workaround: There is no workaround.

- CSCtz14980
Symptoms: When you perform the RP switch, the standby RP (original active one) will keep rebooting.
Conditions: The symptom is observed when you have “crypto map GETVPN_MAP gdoi fail-close” configured and image is Cisco IOS XE Release 3.6 or 3.7.
Workaround: There is no workaround.

- CSCtz25953
Symptoms: “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.
Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.
Workaround: There is no workaround.

- CSCtz35999
The Cisco IOS Software Protocol Translation (PT) feature contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.
Cisco has released free software updates that address this vulnerability.
Workarounds that mitigate this vulnerability are available.
This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-pt
Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.
Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- CSCtz42421
Symptoms: The device experiences an unexpected crash.
Conditions: This symptom is observed when Zone-Based Firewalls are enabled. H225 and H323 inspection is being done during the crash. The actual conditions revolving around the crash is still being investigated.
Workaround: There is no workaround.

- CSCtz47309
Symptoms: When using smart defaults in flexVPN, the mode transport may be sent from initiator even if “tunnel” is configured.
Conditions: First seen on a Cisco ASR that is running Cisco IOS Release 15.2(2)S and a Cisco ISR running Cisco IOS Release 15.2(3)T. It is seen with flexVPN.
Workaround: Use smart defaults on both sides on of the tunnel.

- **CSCtz47595**
  Symptoms: Dial string sends digits at incorrect times.
  Conditions: The symptoms are seen with a Cisco 3925 router running Cisco IOS Release 15.2(3)T using PVDM2-36DM modems with firmware version 3.12.3 connecting over an ISDN PRI to an analog modem.
  When using a dial string to dial an extension (or other additional digits), the modem should answer before the dial string is sent. If a comma is used, there should be a pause after connecting before sending the digits. The default value of the digital modem is one second per comma; two commas would be two seconds, three commas = three seconds and so on.
  1. With any number of commas in the string, debugs show the digits are sent at random intervals, sometimes before the call was answered and as much as up to 30 seconds after the call connects, i.e.: 919195551212x,22 or 1212x,,,22.
  2. With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, i.e.: 919195551212x22.
  Dialing directly to a number with no extension or extra digits works as expected.
  Workaround: There is no workaround.

- **CSCtz72390**
  Symptoms: The name mangling functionality is broken. Authorization fails with the “IKEv2:AAA group author request failed” debug message.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.
  Workaround: There is no workaround.

- **CSCtz73836**
  Symptoms: The router crashes.
  Conditions: This symptom is observed when the router is running NHRP.
  Workaround: There is no workaround.

- **CSCtz78194**
  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.
  Conditions: The symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.
  Workaround: Shorten the ISAKMP profile name to less than 31.

- **CSCtz86763**
  Symptoms: Sessions remain partially created, and memory is consumed and not returned.
  Conditions: This symptom occurs when sessions are churned and reset before they reach active state.
  Workaround: There is no workaround.

- **CSCtz90154**
  Symptoms: Rapid getVPN re-registration by GM when IPsec failure occurs during initial registration. Multiple ISAKMP SAs created and deleted per second.
  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.2(1)S or Release 15.2(1)S2 as a GM.
Workaround: There is no workaround.

- **CSCtz98066**
  Symptoms: When the master switch (Switch A) is reloaded or loses power and rejoins the stack as a member switch, any traffic stream being sent through Switch A is unable to be received by the destination because the newly joined member is not able to establish an ARP entry for the next hop router/switch. Debugs confirm that Switch A does not send a GARP/ARP for the next hop, though traffic continues to be sent to the switch.
  Conditions: The symptom is observed when only Switch A has a physical connection between the source and destination router/L3 switch. The newly elected master (Switch B) does not.
  Workaround: Ping destination from Switch A, forcing ARP request/response.

- **CSCua12317**
  Symptoms: The Cisco 3900 router resets when configuring Object Group/ACL when there is traffic on the interface where an ACL match is needed.
  Conditions: This symptom is observed with the following conditions:
  1. The ACL definition should have service OG ACE.
  2. Reconfigure the service OG ACE or delete it.
  3. Traffic should be passing on the interface where the OG is applied when the above operation is performed.
  Workaround:
  1. Configure a new ACL with the changes needed and apply it to the interface of interest, instead of modifying the already applied one. This is recommended when configuration change is needed.
  2. Remove ACL checks on the interface when changing the configuration (“no ip access-group..”).

- **CSCua12396**
  Symptoms: IPv6 multicast routing is broken when we have master switchover scenarios with a large number of members in stack. Issue is seen on platforms like Cisco 3750E and Cisco 3750X where IPv6 multicast routing is supported.
  Conditions: This symptom is observed when IPv6 multicast routing is configured, mcast routes are populated and traffic is being forwarded. Now, in case of master switchover, synchronization between master and members is disrupted. This is seen only for IPv6 multicast routing. Observed the issue with 9-member stack and either during first or second master switchover. No issues are seen for IPv4 multicast routing.
  Workaround: Tested with 5-member stack, and no issues are seen. It is recommended to enable IPv6 multicast routing when there is deployment with low members in stack.

- **CSCua13848**
  Symptoms: The Cisco ASR 1000 crashes.
  Conditions: This symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.
  Workaround: There is no workaround.

- **CSCua22789**
  Symptoms: Router crashes while doing on-demand image download to switch which does not support Smart Install feature.
Conditions: Router crashes while using CLI to upgrade the images on switch which does not support Smart Install feature.

Workaround: There is no workaround.

- **CSCua23217**
  Symptoms: Ping failure observed.
  Conditions: The symptom is observed with DSL group pairs configured on controllers.
  Workaround: There is no workaround.

- **CSCua24689**
  Symptoms: Fragments are sent without label resulting in packet drops on the other side.
  Conditions: The symptom is observed with the following conditions:
  - MPLS enabled DMVPN tunnel on egress.
  - VFR on ingress.
  Workaround: Disable VFR if possible.

- **CSCua29095**
  Symptoms: Spurious memory access is seen when booting the image on a Cisco 7600 router.
  Conditions: This symptom occurs while booting the image.
  Workaround: There is no workaround.

- **CSCua39107**
  Symptoms: In a FlexVPN Spoke-to-Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.
  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.
  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- **CSCua39390**
  Symptoms: The PRI configuration (voice port) is removed after a reload:

  ```
  interface Serial1/0:23 ^
  % Invalid input detected at '^' marker. 
  no ip address % Incomplete command. 
  encapsulation hdlc ^
  % Invalid input detected at '^' marker. 
  isdn incoming-voice voice ^
  % Invalid input detected at '^' marker. 
  no cdp enable ^
  % Invalid input detected at '^' marker. 
  voice-port 1/0:23 ^
  % Invalid input detected at '^' marker. 
  Also getting trace back:
  %SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
  -Traceback= 0x607E01Cz 0x630F0478z 0x607F72C0z 0x607222F38z 0x6070A300z
  0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
  0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
  ```
%SYS-2-INTSCHED: 'may_suspend' at level 3  - Process= "Init", ipl= 3, pid= 3  
-Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154zz

Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T and Release 15.1(4)M4. The issue is not occurring with Cisco IOS Release 12.4(24)T6 or lower. The issue occurs after reload.

Workaround: Reapply configuration after router comes back up.

- CSCua55629

Symptoms: SIP memory leak seen in the event SIPSPI_EV_CC_MEDIA_EVENT.

Conditions: The command show memory debug leaks shows a CCSIP_SPI_CONTROL leak with size of 6128 and points to the event “SIPSPI_EV_CC_MEDIA_EVENT?”:

Adding blocks for GD...

I/O memory

<table>
<thead>
<tr>
<th>Address</th>
<th>Size</th>
<th>Alloc_pc</th>
<th>PID</th>
<th>Alloc-Proc</th>
<th>Name</th>
</tr>
</thead>
</table>

Processor memory

<table>
<thead>
<tr>
<th>Address</th>
<th>Size</th>
<th>Alloc_pc</th>
<th>PID</th>
<th>Alloc-Proc</th>
<th>Name</th>
</tr>
</thead>
</table>

Workaround: There is no workaround.

- CSCua55785

Symptoms: Build breakage due to fix of CSCtx34823.

Conditions: This issue occurs with CSCtx34823 fix.

Workaround: CSCtx34823 change may be unpatched from the code-base.

- CSCua61330

Symptoms: Traffic loss is observed during switchover if,

1. BGP graceful restart is enabled.
2. The next-hop is learned by BGP.

Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.

Workaround: There is no workaround.

- CSCua65278

Symptoms: Modem disappears with the cellular 0 cdma mode evdo command.

Conditions: The symptom is observed with the cellular 0 cdma mode evdo command when loaded with Cisco IOS interim Release 15.3(0.4)T.

Workaround: There is no workaround.

- CSCua75069

Symptoms: BGP sometimes fails to send an update or a withdraw to an iBGP peer (missing update)

Conditions: This symptom is observed only when all of the following conditions are met:

1. BGP advertise-best-external is configured, or diverse-path is configured for at least one neighbor.
2. The router has one more BGP peers.
3. The router receives an update from a peer, which changes an attribute on the backup path/repair path in a way which does not cause that path to become the best path.

4. The best path for the net in step #3 does not get updated.

5. At least one of the following occurs:
   - A subsequent configuration change would cause the net to be advertised or withdrawn.
   - Dampening would cause the net to be withdrawn.
   - SOO policy would cause the net to be withdrawn.
   - Split Horizon or Loop Detection would cause the net to be withdrawn.
   - IPv4 AF-based filtering would cause the net to be withdrawn.
   - ORF-based filtering would cause the net to be withdrawn.
   - The net would be withdrawn because it is no longer in the RIB.

The following Cisco IOS releases are known to be impacted if they do not include this fix:
   - Cisco IOS Release 15.2T and later releases
   - Cisco IOS Release 15.1S and later releases
   - Cisco IOS Release 15.2M and later releases
   - Cisco IOS Release 15.0EX and later releases

Older releases on these trains are not impacted.

Workaround: If this issue is triggered by a configuration change, you can subsequently issue the `clear ip bgp neighbor soft out` command.

- CSCua78782
  Symptoms: Authentication of EzVPN fails.
  Conditions: The symptom is observed with BR-->ISP-->HQ.
  Workaround: There is no workaround.

- CSCua93001
  Symptoms: Auto-RP group is not automatically joined upon bootup.
  Conditions: The symptom is observed when the router reboots and starts from the existing configurations.
  Workaround: Manually re-enable “ip pim autorp” after bootup.

- CSCua96106
  Symptoms: MSP is not enabled on Cisco 890 platform images.
  Conditions: This symptom is observed when the `profile flow` global command is not available.
  Workaround: There is no workaround.

- CSCua99969
  Symptoms: IPv6 PIM null-register is not sent in the VRF context.
  Conditions: This symptom occurs in the VRF context.
  Workaround: There is no workaround.

- CSCub19471
  Symptoms: Crash during boot up with MACE and SNMP configurations.
Conditions: The symptom is observed when the startup configuration contains MACE type (policy-map type mace) configured with both filter (match access-group) and action (e.g. flow monitor). The SNMP configuration is as follows:

```plaintext
flow record type mace mace-record
  collect art all
!
flow exporter ndeget
  destination 172.25.215.96
!
flow monitor type mace mace-monitor
  record mace-record
!
!
class-map match-all mace-class
  match access-group name mace-acl
!
policy-map type mace mace_global
  class mace-class
    flow monitor mace-monitor
!
interface e0/0
  mace enable

ip access-list extended mace-acl
  permit tcp any any
!
snmp-server community public RO
snmp-server community cisco RW
snmp-server ifindex persist
snmp mib persist cbqos
snmp mib persist circuit
```

Reload the router, then during router boot up there will be a crash.

Workaround: Remove SNMP configuration.

- **CSCub30751**
  
  Symptoms: DNS SRV based SIP calls fail even though the router is able to resolve the DNS SRV.

  Conditions: None.

  Workaround: Static IP host entry in the router configuration

- **CSCub54872**
  
  Symptoms: A /32 prefix applied to an interface (e.g.: a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.

  Conditions: The symptom is observed when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).

  Workaround: Use a shorter prefix.

  Further Problem Description: This issue does not affect software switching platforms.

- **CSCub55790**
  
  The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. Affected devices that are configured as Smart Install clients are vulnerable.
Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall

- CSCub69976
  Symptoms: Cisco 1941 in a DMVPN setup crashes with Cisco IOS Release 15.2(2)T2. The Cisco 2911 router and the Cisco 3945 router crash in a FlexVPN setup running Cisco IOS Release 15.3(00.14)T.
  Conditions: This symptom occurs in a DMVPN setup and in the FlexVPN setup.
  Workaround: Disable the ISM module and switch to the onboard crypto engine using “no crypto engine slot 0”.

- CSCub70336
  Symptoms: The router can crash when “clear ip bgp *” is done in a large-scale scenario.
  Conditions: This symptom is observed only in a large-scale scenario, with ten of thousands of peers and several VPNv4/v6 prefixes.
  Workaround: “clear ip bgp *” is not a very common operation. Hence, this issue has not been observed by customers. The crash can only happen when “clear ip bgp *” is done. The workaround is not to execute “clear ip bgp *”.

- CSCub76103
  Symptoms: When callback tries to send message there is traceback.
  Conditions: The symptom is observed when you set the call-home profile’s transport to HTTP and but you do not set the HTTP address.
  Workaround: When you set the call-home profile’s transport to HTTP, ensure the HTTP address value is also set correctly. For example, in call-home profile mode:
  destination address http https://example.xxx.xxx

- CSCub84471
  Symptoms: WAAS-optimized traffic is stuck in a loop when ISM VPN is enabled.
  Conditions: This symptom occurs when the ISM-VPN Module is turned on.
  Workaround: There is no workaround.

- CSCub86706
  Symptoms: After multiple RP switchover, the router crashes with the “UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO” error.
  Conditions: This symptom is observed with MVPN with 500 VRFs, when performing multiple switchovers on PE1.
  Workaround: There is no workaround.

- CSCub90459
  Symptoms: If CUBE has midcall reinvite consumption enabled, it also consumes SIP 4XX responses. This behavior can lead to dropped or hung calls.
  Conditions: This symptom occurs when midcall reinvite consumption is enabled.
  Workaround: There is no workaround.

- CSCuc06307
Symptoms: When an L2TPv3 xconnect with IP interworking is configured on a Switched Virtual Interface (interface vlan), it may fail to pass traffic. With debug subscriber packet error enabled, debug messages like the following are output:

```
AC Switching[Vl10]: Invalid packet rcvd in process path, dropping packet
```

Conditions: This symptom has been observed in Cisco IOS Release 15.2(3)T4 and earlier.

Workarounds:
- There is no workaround.

**CSCuc14674**

Symptoms: In a GetVPN configuration, when utilizing the ISM VPN module, traffic does not pass even though IPsec SAs are up when CEF is enabled, and “ip traffic-export” is configured in the crypto map interface.

Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T1 or later releases, and when CEF is enabled. This issue is seen when “ip traffic-export” is configured in the crypto map interface, and ISM is the crypto engine.

Workarounds:
1. Disable CEF.
2. Do not configure “ip traffic-export” in the crypto map interface.
3. Disable ISM using “no cry engine slot 0”. Then, the onboard engine will be used.

**CSCuc19046**

Symptoms: Active Cisco IOSd was found to have crashed following the “clear ip mroute *” CLI.

Conditions: This symptom occurs with 4K mroutes (2k *,G and 2K S,G) running the FFM performance test suite.

Workarounds:
- There is no workaround.

Further Problem Description: So far, this issue is only seen in the FFM performance test script.

**CSCuc42518**

Symptoms: Cisco IOS Unified Border Element (CUBE) contains a vulnerability that could allow a remote attacker to cause a limited Denial of Service (DoS). Cisco IOS CUBE may be vulnerable to a limited Denial of Service (DoS) from the interface input queue wedge condition, while trying to process certain RTCP packets during media negotiation using SIP.

Conditions: Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when certain sequence of RTCP packets is processed. All the calls on the affected interface would be dropped.

Workarounds:
- Increase the interface input queue size. Disable Video if not necessary.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/3.1:


CVE ID CVE-2012-5427 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:


**CSCuc55634**

Symptoms: IPv6 static route cannot resolve the destination.

Conditions:
1. A VRF is configured by the old style CLI (for example “ip vrf RED”).
2. Configure “ip vrf forwarding RED” under an interface.
3. Configure IPv6 address under the same interface (for example 2001:192:44:1::2/64).


5. Then, we are not able to ping the 2001:192:14:1::2 although we can reach 2001:192:44:1::1.

Workaround: There is no workaround.

- CSCuc56259

Symptoms: A Cisco 3945 that is running 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen:

%VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times and Delivery Ack could not be sent due to lack of buffers.

Conditions: This happens when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

Workaround: Check the configurations for any misconfigurations, especially with calls involving CUBE and CUCM.

- CSCuc67033

Symptoms: A Cisco IOS router with the ISM VPN encryption module enabled can experiences memory corruption-related crashes.

Just before the crash, the router may display some syslog error messages related to the ISM VPN module:

Aug 21 15:55:22: !!! Cannot find Revt counters struct for flowid: 0x4400012A
Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A
Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A

Here, the word "Revt" is specific for the ISM VPN module.

Also, some generic syslog error messages related to memory allocation failures may be displayed the crash:

Aug 21 15:55:33: %SYS-3-BADBLOCK: Bad block pointer DD7D7D0
-Traceback= 23B9BB7Cz 23BA1A44z 23BA1E24z 23B7128Bz 23B7129Cz
352791C4, 22DB4A50 352791C4, 3000006C 38808760, 2627EDF0 34C91824, 262724A8
352791C4, 22DB6214 352791C4, 3000006C 352791C4, 22DB6214
352791C4, 22DB4A50 352791C4, 3000006C 352791C4, 22DB6214 3875D9C4, 600002CA
3875D9C4, 2627EDF0 35092ACC, 262724A8 352791C4, 22DB4A50 352791C4, 3000006C
Aug 21 15:55:33: %SYS-6-BLKINFO: Corrupted next pointer blk DD7D7D0, words 32808, alloc 214E636C, InUse, dealloc 0, rfcnt 1

Conditions: This symptom is observed with the following conditions:

- The ISM VPN crypto acceleration module is installed, enabled, and used for crypto operations (IPsec, etc.).

- Cisco IOS supports ISM VPN (Cisco IOS Release 15.2(1)T1 or later releases).

Workaround: Disable the ISM VPN module. The crash is specific to ISM VPN.

- CSCuc69342

Symptoms: About 10 minutes after CUBE boot, the router crashes with the following traceback:

-Traceback= 5B01805 46158ED 45F4F37 45BB19E 45BA1CF 451D6DC 45255594 45252D9 4519C30 45196A9 4778FFD

After the reload from the crash, it may take some time before it crashes again.
Conditions: This symptom occurs when CUBE receives the SIP REFER message with the Refer-To header having no user part.

Workaround: There is no workaround.

- CSCuc82992
  Symptoms: The router crashes upon execution of “no crypto engine slot 0”. when RG-infra feature is enabled.
  Conditions: This symptom occurs when RG-Infra and ISM-VPN are configured and when issuing “no crypto engine slot 0”.
  Workaround: There is no workaround.

- CSCuc94508
  Symptoms: The router crashes in NBAR Flowvar ch chunk.
  Conditions: This symptom occurs when the router is configured with NBAR features.
  Workaround: Disable NBAR-related commands.

- CSCud01502
  Symptoms: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.
  Conditions: This symptom occurs in CME.
  Workaround: There is no workaround.

- CSCud03273
  Symptoms: All the paths using certain next-hops under the route-map are marked inaccessible.
  Conditions: This symptom occurs under the following conditions:
  1. Configure peer groups.
  2. Apply BGP NHT with route-map (no BGP neighbors are created or added to peer groups).
  3. Configure the Prefix-list.
  4. Configure the route-map.
  5. Configure the BGP neighbor and add them to peer groups.
  Workaround: Configure “route-map permit <seq-num> <name>” or activate at least one neighbor in “address-family ipv4”.

- CSCud22222
  Symptoms: On a router running two ISIS levels and fast-reroute, the router may crash if “metric-style wide level-x” is configured for only one level.
  Conditions: Issue may happen if metric-style wide is configured for only one level on router running both levels, and fast-reroute is configured.
  Workaround: Configure metric-style wide for both levels (by default).

- CSCud33159
  Symptoms: Excessive loss of MPLS VPN traffic and high CPU utilization is observed due to the process switching of MPLS traffic over the ATM interface.
  Conditions: This symptom occurs when MPLS is enabled on the ATM interface with aal5snap encapsulation.
  Workaround: There is no workaround.

- CSCud64812
A vulnerability in the implementation of the virtual fragmentation reassembly (VFR) feature for IP version 6 (IPv6) in Cisco IOS Software could allow an unauthenticated, remote attacker to cause an affected device to hang or reload, resulting in a denial of service (DoS) condition.

The vulnerability is due to a race condition while accessing the reassembly queue for IPv6 fragments. An attacker could exploit this vulnerability by sending a crafted stream of valid IPv6 fragments. Repeated exploitation may result in a sustained DoS condition.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability.

This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ipv6-vfr

Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- CSCud67792
  Symptoms: An invalid modem is detected.
  Conditions: This symptom is observed during bootup.
  Workaround: Use Cisco IOS Release 15.2T-based images.

- CSCud94557
  Symptoms: Build failed to compile c800 images.
  Conditions: The symptom is observed with c800 images.
  Workaround: There is no workaround.

- CSCue05844
  Symptoms: The Cisco 3925 router running Cisco IOS Release 15.0(2)SG reloads when connecting to a call manager.
  Conditions: This symptom is observed with the Cisco 3925 router running Cisco IOS Release 15.0(2)SG.
  Workaround: Remove SNMP.

Resolved Bugs—Cisco IOS Release 15.2(3)T2

Cisco IOS Release 15.2(3)T2 is a rebuild release for Cisco IOS Release 15.2(3)T. The bugs in this section are resolved in Cisco IOS Release 15.2(3)T2 but may be open in previous Cisco IOS releases.

- CSCsi02145
  Symptoms: A Cisco router may stop processing traffic on an interface that is configured with VRF Lite.
  Conditions: This symptom is observed when the input queue eventually wedges (76/75) below due to ICMP redirect messages being stuck.
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 5475.d0e0.1da8 (bia 5475.d0e0.1da8)
  Description: to Switch
  Internet address is x.x.x.x/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:02:01, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:32:15
  Input queue: 76/75/117/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo

Workaround: Locate the source of the ICMP redirects and address the underlying reason they are being sent to the router.

- CSCtr45287
  Symptoms: The router crashes in a scale DVTI scenario.
  Conditions: This symptom is observed when the IPsec tunnel count reaches around 2500.
  Workaround: Use fewer tunnels or use a different platform.

- CSCts68626
  Symptoms: PPPoE discovery packets causes packet drop.
  Conditions: This symptom is observed when you bring up a PPPoE session and then clear the session.
  Workaround: There is no workaround.

- CSCts83046
  Symptoms: Back-to-back ping fails for P2P GRE tunnel address.
  Conditions: This symptom is observed when HWIDB is removed from the list (through list remove) before it gets dequeued.
  Workaround: There is no workaround.

- CSCtu40028
  Symptoms: The SCHED process crashes.
  Conditions: This symptom occurs after initiating TFTP copy.
  Workaround: There is no workaround.

- CSCtv36812
  Symptoms: Incorrect crashInfo file name is displayed during crash.
  Conditions: This symptom is observed whenever a crash occurs.
  Workaround: There is no workaround.

- CSCtw46229
  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.
  Conditions: This symptom is observed with PPP negotiations and the session involving PPPoA.
  Workaround: Ensure that all your PPP connections stay stable.
- **CSCtw55976**
  Cisco IOS Software contains a vulnerability in the Intrusion Prevention System (IPS) feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist.
  
  Cisco has released free software updates that address this vulnerability.
  Workarounds that mitigate this vulnerability are available.
  
  This advisory is available at the following link:

- **CSCtw88689**
  Symptoms: A crash is seen while applying the policy map with more than 16 classes with the Cisco 3900e platform.
  
  Conditions: This symptom occurs when applying the policy map with more than 16 classes.
  Workaround: There is no workaround.

- **CSCtw98200**
  Symptoms: Sessions do not come up while configuring RIP commands that affect the virtual-template interface.
  
  Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS.
  
  RIP is configured with the `timers basic 5 20 20 25` command. Also, every interface matching the network statements is automatically configured using the `ip rip advertise 5` command. These interfaces include the loopback and virtual-template interfaces too.
  
  On a Cisco ASR1000 series router, this configuration causes the creation of full VAs which are not supported. Hence, the sessions do not come up. On Cisco ISR 7200 routers, VA subinterfaces can be created.
  
  Workaround: Unconfigure the `timers rip` command.

- **CSCtx17480**
  Symptoms: The router crashes when trying to free the received LCP CONF Request packet containing the option that is not recognizable or is not acceptable for negotiation and the CONF reject for that option is sent.
  
  Conditions: This symptom occurs when the option that is not recognizable or is not acceptable for negotiation is of length 0 or invalid length.
  
  Workaround: There is no workaround.

- **CSCtx22322**
  Symptoms: If an over-temperature interrupt occurs when the CPU utilization is high, the system may crash.
  
  Conditions: This symptom is observed when CPU utilization of the system is high Cisco 880 series routers.
  
  Workaround: There is no workaround.

- **CSCtx48753**
  Symptoms: Higher memory usage with PPP sessions than seen in Cisco IOS XE Release 3.4/3.5.
  
  Conditions: This symptom is observed with configurations with PPP sessions. These will see up to 10% higher IOS memory usage than in previous images.
  
  Workaround: There is no workaround.
Bugs for Cisco IOS Release 15.2(3)T

- **CSCtx66011**
  A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.

  The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).

  Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.

  In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.

  Only IKEv1 is affected by this vulnerability.

  An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:


  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:


- **CSCtx66046**

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers the address of the loopback interface.

- **CSCtx66804**

  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.

  Conditions: The symptom is observed with the following conditions:

  - “ppp lcp delay 0” is configured.
  - Cisco IOS Release 15.0(1)M5.

  Workaround: Set delay timer without 0.
- CSCtx95840
  Symptoms: A Cisco voice gateway may unexpectedly reload.
  Conditions: This symptom is observed on a Cisco voice gateway running SIP protocol. In this case, the issue occurs when sipSPIUfreeOneCCB() returns, and the leftover event is still being processed after CCB is released from sipSPIUfreeOneCCB(). Based on sipSPIStartRemoveTransTimer(ccb), CCB should have been released later by a background timer.
  Workaround: There is no workaround.

- CSCty01237
  Symptoms: The router logs show:
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED
  CMD: 'show run' <timestamp>
  This is followed by the router crashing.
  Conditions: This issue is seen under the following conditions:
  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes show run on the MC over HTTP or some other means.
  Workaround 1: If you use the PfR learn-list feature, do not execute show run periodically.
  Workaround 2: If you use a monitoring tool that executes show run periodically, avoid using a learn-list configuration in PfR.

- CSCty04359
  Symptoms: In a manually created WExp device certificate, when the image is upgraded from Cisco IOS Release 15.1(3)T (Phase 1) to Cisco IOS Release 15.2(3)T (Phase 2), the device goes offline in WCM.
  Conditions: This symptom is observed with a manually created WExp device certificate, when the image is upgraded from Cisco IOS Release 15.1(3)T (Phase 1) to Cisco IOS Release 15.2(3)T (Phase 2).
  Workaround: Configure the trustpoint policy using rsakeypair, and add the rsakeypair trustpoint-name command to the configuration.

- CSCty32851
  Symptoms: A Cisco router may unexpectedly reload due to a software forced crash exception when changing the encapsulation on a serial interface to “multilink ppp”.
  Conditions: This symptom is observed when the interface is configured with a VRF.
  Workaround: Shut down the interface before making the encap configuration change.

- CSCty48870
  Symptoms: The router crashes due to a bus error.
  Conditions: This symptom has been observed in a router that is running Cisco IOS Release 15.2(2)T and Cisco IOS Release 15.2(3)T with NBAR enabled on a crypto-enabled interface. NBAR can be enabled through NAT, QoS, or NBAR protocol discovery.
  Workaround: Using no ip nat service nbar will help where NBAR is enabled through NAT.

- CSCty51453
  Symptoms: Certificate validation using OCSP may fail, with OCSP server returning an “HTTP 400 - Bad Request” error.
Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T2 and later.

Workaround 1: Add the following commands to change the TCP segmentation on the router:

```console
router(config)# ip tcp mss 1400
router(config)# ip tcp path-mtu-discovery
```

Workaround 2: Use a different validation method (CRL) when possible.

- **CSCty54695**

  Symptoms: RRI routes are missing when IPsec SA is up after peer IP change.

  Conditions: This symptom is observed under the following conditions:
  - Cisco ASR 1002 router running Cisco IOS XE Release 3.4.2S.
  - Dynamic crypto map with RRI.
  - Peer changes the IP address frequently.

  Workaround: Clear the crypto session with the peer.

- **CSCty55449**

  Symptoms: The device crashes after registering an Embedded Event Manager TCL policy.

  Conditions: This symptom occurs if the policy uses the multiple event feature and the trigger portion is registered without curly braces ("{}"). Then, the device will crash. For example, this policy will trigger a crash:

  ```console
  ::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
  ::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
  ::cisco::eem::trigger
  ::cisco::eem::correlate event 1 or event 2
  namespace import ::cisco::eem::*
  namespace import ::cisco::lib::*
  action_syslog priority crit msg " triggered "
  ``

  Note how "::cisco::eem::trigger" is not followed by an opening curly brace.

  Workaround: Ensure that the trigger portion (that is, the correlate statement) is enclosed within curly braces. Given the example above, the proper syntax is:

  ```console
  ::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
  ::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
  ::cisco::eem::trigger {
   ::cisco::eem::correlate event 1 or event 2
  }
  namespace import ::cisco::eem::*
  namespace import ::cisco::lib::*
  action_syslog priority crit msg " triggered "
  ``

- **CSCty56850**

  Symptoms: Routers are not updating the cnpdAllStatsTable with traffic from all expected protocols.

  Conditions: This symptom is observed with routers that are running Cisco IOS 15.x (tested in 15.0, 15.1, and 15.2(2)T).

  Workaround 1: Use the following CLI to get the stats for all the protocols:

  ```console
  show IP NBAR protocol-discovery
  ```
Workaround 2: Perform a snmpget against objects in cnpdAllStatsTable.

- **CSCty64721**
  
  Symptoms: Improper memory allocation by CTI process crashes the CME.

  Conditions: This symptom occurs when the CTI front end process is using up huge memory, causing the CME to crash eventually. When the crash occurs:

  Processor Pool Total: 140331892 Used: 140150164 Free: 181728
  I/O Pool Total: 27262976 Used: 5508116 Free: 21754160

  Workaround: There is no workaround.

- **CSCty65189**
  
  Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

  Conditions: This symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- **CSCty80553**
  
  Symptoms: A multicast router crashes.

  Conditions: This symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.

  Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- **CSCty86039**
  
  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.

  Conditions: This symptom is seen with tunnel interface with QoS policy installed.

  Workaround: There is no workaround.

- **CSCty96052**
  
  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: This symptom is an extreme corner case/timing issue. This issue has been observed only once on a release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- **CSCty97961**
  
  Symptoms: A device configured with SSLVPN crashes.

  Conditions: This symptom is observed when a device configured is with SSLVPN and **functions svc-enabled** or **functions svc-required** and **svc dtls**, and has an outbound ACL on one of the device’s interface.

  This vulnerability has only been observed when the outbound ACL is tied to either a NAT or ZBFW interface in the outbound direction and is not the interface that the SSLVPN session is terminated against.

  This vulnerability has only been observed when the SSLVPN sessions terminate over PPP over the ATM interface.

  This vulnerability was not able to be reproduced over SSLVPN sessions terminating over Ethernet or Serial interfaces.
Workaround: Remove the outbound ACL, or **no svc dtls** if running Cisco IOS software that has a fix for CSCte41827.

Further Problem Description: This bug covers configurations that have DTLS enabled on the device. A corresponding Cisco Bug ID, CSCte41827, deals with a similar vulnerability but when the device does not have DTLS configured.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:


CVE ID CVE-2012-3924 has been assigned to document this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:


- **CSCtz13465**
  
  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.
  
  Conditions: This symptom is observed with an interface with a policy installed.
  
  Workaround: There is no workaround.

- **CSCtz13818**
  
  Symptoms: In a rare situation when route-map (export-map) is updated, Cisco IOS is not sending refreshed updates to the peer.
  
  Conditions: This symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then, Cisco IOS does not send refreshed updates with modified route-targets.
  
  Workaround 1: Refresh the updated route-target to use `clear ip route vrf vrf-name net mask`.
  
  Workaround 2: Hard clear the BGP session with the peer.

- **CSCtz26735**
  
  Symptoms: The SDP process to provision the CVO router is broken in Cisco IOS Release 15.2(3)T.
  
  Conditions: This symptom is seen when we start the SDP process. The connection immediately breaks after the username and password are entered.
  
  Workaround: There is no workaround.

- **CSCtz37164**
  
  Symptoms: The requests to the RADIUS server are retransmitted even though the session no longer exists, causing unnecessary traffic to RADIUS, and RADIUS getting requests for an invalid session.
  
  Conditions: This symptom occurs when the RADIUS server is unreachable and the CPE times out the session.
  
  Workaround: The fix is currently being worked upon. This issue can be seen as per the conditions mentioned above. This issue can be avoided by making sure that the RADIUS server is always reachable.

- **CSCtz37863**
  
  Symptoms: IPCP is not in an open state and it does not seem to be calling the This-Layer-Down (TLD) vector.
  
  Conditions: This symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.
  
  Workaround: There is no workaround.
Bugs for Cisco IOS Release 15.2(3)T

- CSCtz44989
  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.
  Conditions: This symptom is observed with IPv6 link-local next-hop. When the EIGRP route is redistributed to BGP VRF, it clears the next-hop information (it becomes 0.0.0.0). Then, this route becomes invalid and BGP is not able to export to another VRF.
  Workaround: There is no workaround.

- CSCtz58719
  Symptoms: Watchdog timeout is seen under interrupt or process.
  Conditions: This symptom is observed with a QoS configuration applied. This issue happens because of resource contention between a process path packet and an interrupt path packet.
  Workaround: Disable QoS.

- CSCtz58941
  Symptoms: The router crashes when users execute the `show ip route XXXX` command.
  Conditions: This symptom is observed during the display of the `show ip route XXXX`, when the next-hops of “XXXX” networks are removed.
  Workaround: The `show ip route XXXX` command (without “XXXX”) does not have the problem.

- CSCtz59145
  Symptoms: A crash occurs randomly. The following error messages are often seen before the crash:

  Mar 31 16:30:16.955 GMT: %SYS-2-MALLOCFAIL: Memory allocation of 20 bytes failed from 0x644DA7E0, alignment 0
  Pool: Processor Free: 274176384 Cause: Interrupt level allocation
  Alternate Pool: None Free: 0 Cause: Interrupt level allocation
  -Process= '<interrupt level>', ipl= 1

  Mar 31 16:30:16.963 GMT: %SYS-3-BADLIST_DESTROY: Removed a non-empty list(707C0248, name: FW DP SIP dialog list), having 0 elements

  This device is not actually running out of memory. There is a memory action going on at the interrupt level which is not allowed.

  Conditions: This symptom occurs when Zone-Based Firewalls inspect SIP traffic. This issue is likely related to the tracebacks and error messages given above. The actual condition is still being investigated.
  Workaround: If plausible, disabling SIP inspection could possibly prevent further crashes.

- CSCtz70623
  Symptoms: A Cisco router may experience a software-forced crash.
  Conditions: This symptom occurs when a two-wire cable is unplugged from the G.SHDSL interface.
  Workaround: There is no workaround.

- CSCtz71084
  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.
  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

  CE0------------------PE0---------------------RR
Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y

Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

Workaround: Hard clear.

- CSCtz72044
  Symptoms: The EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.
  Conditions: This symptom is timing-dependent; therefore, the problem is not systematic.
  Workaround: There is no workaround.

- CSCtz73263
  Symptoms: MSP is not getting packets on SVI interface and MSP profile is not getting attached to the flow.
  Conditions: This symptom is observed when the profile flow command is configured globally and an MSP profile is applied using media-proxy services profile-name.
  Workaround: Disable MSP using no profile flow and enable it again using profile flow.

- CSCtz77171
  Symptoms: Subscriber drops are not reported in mod4 accounting.
  Conditions: This symptom is observed on checking the policy-map interface for account QoS statistics on a port-channel subinterface.
  Workaround: There is no workaround.

- CSCtz80643
  Symptoms: A PPPoE client’s host address is installed in the LNS’s VRF routing table with the ip vrf receive vrf name command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.
  Conditions: This symptom is observed only when the Virtual-access interface is configured with the ip vrf receive vrf name command via the Virtual-Template or RADIUS profile.
  Workaround: There is no workaround.

- CSCua06598
  Symptoms: The router may crash with breakpoint exception.
  Conditions: This symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally sourced BGP route installed in IPv6 RIB.
  Workaround: Disable SNMP IPv6 polling.
- **CSCua07791**
  Symptoms: A Cisco ISR G2 running Cisco IOS Release 15.2(2)T or later shows a memory leak in the CCSIP_SPI_CONTRO process.
  Conditions: This symptom is observed when the leak is apparent after 3-4 weeks. The process is CCSIP_SPI_CONTRO.
  Workaround: There is no workaround.

- **CSCua15292**
  Symptoms: The router may report unexpected exception with overnight stress traffic.
  Conditions: This symptom is observed with the following conditions:
  - Cisco ISR 3925E is deployed as DMVPN hub router and about 100Mbps traffic is controlled by PfR MC with dynamic PBR.
  - Router logs with %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec’d IPSEC packet has invalid spi for destaddr=172.8.9.8, prot=50, spi=0xE8FB045F(3908764767), srcaddr=10.0.100.1, input interface=GigabitEthernet0/0
  Workaround: There is no workaround.

- **CSCua31157**
  Symptoms: One-way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. Issue is only seen intermittently.
  Logs on the spoke that fails to receive the traffic show “Invalid SPI” error messages exactly 1 minute after the tunnel between the spokes came up.
  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T1.
  Workaround: There is no workaround.

- **CSCua33821**
  Symptoms: CPU utilization shoots up to 99% after configuring crypto maps.
  Conditions: This symptom is observed after applying crypto maps.
  Workaround: There is no workaround.

- **CSCua40273**
  Symptoms: The Cisco ASR 1000 series router crashes when displaying MPLS VPN MIB information.
  Conditions: This symptom occurs on the Cisco ASR 1000 series router running Cisco IOs Release 15.1(02)S.
  Workaround: Avoid changing the VRF while querying for MIB information.

- **CSCua43930**
  Symptoms: The checksum value parsed from GRE header is not populating, causing the GRE tunnel checksum test case to fail.
  Conditions: This symptom occurs on a Cisco ISR G2.
  Workaround: There is no workaround.

- **CSCua45122**
  Symptoms: Multicast even log preallocated memory space needs to be conserved on the low-end platform.
Conditions: This symptom is observed with multicast even log.
Workaround: There is no workaround.

- CSCua47570
  Symptoms: The **show ospfv3 event** command can crash the router.
  Conditions: This symptom is observed when “ipv4 address family” is configured and redistribution into OSPFv3 from other routing protocols is configured.
  Workaround: Do not use the **show ospfv3 event** command.

- CSCua49764
  Symptoms: The WAAS-Express device goes offline on WCM.
  Conditions: This symptom occurs when a certificate is generated using HTTPS when using the Cisco IOS Release 15.1(3)T image. Once upgraded to Cisco IOS Release 15.2(3)T, the WAAS-Express device goes offline on WCM.
  Workaround: Configure an rsakeypair on the TP-self-signed trustpoint with the same name and execute the **enroll** command again or delete the self-signed trustpoint point and reenable the HTTP secure-server.

- CSCua51991
  Symptoms: An invalid SPI message is seen throughout the lifetime of IPsec SA.
  Conditions: This symptom is observed with SVTI-SVTI with a GRE IPv6 configuration. When bringing up 1K sessions, an invalid SPI is seen. There is also inconsistency between the number of child SAs in IKEv2 and the number of IPsec SAs on the same box.
  Workaround: There is no workaround.

- CSCua60785
  Symptoms: Metadata class-map matches only the first of the following filter, if present, in a class map (the other media-type matches are skipped):

  ```
  match application attribute [category, sub-category, media-type, device-class] value-string
  match application application-group value-string
  ```

  Conditions: This symptom is observed in a case where the class map has the aforementioned filters.
  Workaround: There is no workaround.

- CSCua67998
  Symptoms: The system crashes.
  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.
  Workaround: There is no workaround.

- CSCua71038
  Symptoms: The router crashes.
  Conditions: This symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.
  Workaround: Configure OCSP or CRL but not both
• CSCua77729
Symptoms: Embedded AP in the Cisco 1941 ISR becomes unreachable after using the “reload in” command on the Cisco ISR CLI. This issue is seen when using “reload in” on the Cisco ISR CLI and choosing the option to reload embedded AP.

CISCO1941W-E/K9 Version 15.1(4)M4
AP801 Software (AP801-K9W7-M), Version 12.4(21a)JA1

Router#reload in 10
Do you want to reload the internal AP? [yes/no]: yes
Do you want to save the configuration of the AP? [yes/no]: no
System configuration has been modified. Save? [yes/no]: no
Reload scheduled for 13:57:01 UTC Mon May 21 2012 (in 10 minutes) by console
Reload reason: Reload Command
Proceed with reload? [confirm]
Router#
May 21 13:47:03.759:
%SYS-5-SCHEDULED_RELOAD:<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi?action=search&counter=0&paging=5&links=reference&index=all&query=SYS-5-SCHEDULED_RELOAD>

After that, AP becomes unreachable, and the user cannot session to AP with "service-module wlan-ap 0 session".

Conditions: This symptom is observed when using “reload in” on the Cisco ISR CLI and choosing the option to reload embedded AP. This issue is seen under the following conditions:

CISCO1941W-E/K9 Version 15.1(4)M4
AP801 Software (AP801-K9W7-M), Version 12.4(21a)JA1
using the “reload in” command on ISR CLI with Do you want to reload the internal AP? [yes/no]: yes

Workaround 1: Use “reload in” on the Cisco ISR CLI and do not choose the option to reload embedded AP.
Router#reload in 2
Do you want to reload the internal AP? [yes/no]: no

Workaround 2: Use the normal reload command.

• CSCua84923
Symptoms: Following a misconfiguration on a two-level hierarchical policy with a user-defined queue-limit on a child policy, the UUT fails to attach the QoS policy on the interface even when corrected queueing features are used.

Conditions: This symptom is observed with the following conditions:

1. The issue must have the user-defined queue-limit defined.
2. 2) This error recovery defected is confirmed as a side effect with the c3pl cnh compoent project due to ppcp/cce infras tructure enhancement.

Workaround: There is no workaround.

• CSCua86620
Symptoms: The vmware-view application is not detected/classified.

Conditions: This symptom is observed when vmware-view applications are used.
Workaround: There is no workaround.

- **CSCua93688**
  
  Symptoms: When pinging from the Cisco 1921 router to connected devices, the response time is unexpectedly slow.
  
  $\text{round-trip min/avg/max} = 8/46/92 \text{ ms}$
  
  Conditions: This symptom is observed with the EHWIC-1GE-SFP-CU module on Cisco ISR-G2 platforms.
  
  Workaround: Shut/no shut the EHWIC-1GE-SFP-CU interface. The ping time resumes to normal.

- **CSCua96354**
  
  Symptoms: Reload may occur when issuing the `show oer` and `show pfr` commands.
  
  Conditions: This symptom is observed with the following commands:
  - `show oer master traffic-class performance`
  - `show pfr master traffic-class performance`
  
  Workaround: There is no workaround.

- **CSCua97981**
  
  Symptoms: The Cisco IOS redundancy facility is slow to come up after master router reload and gets stuck in the “final progression” state.
  
  Conditions: This symptom was first seen in Cisco IOS Release 15.2(3)T and was also observed in Cisco IOS Release 15.2(3)T1.
  
  Workaround: Manually reloading the Standby router will resolve the issue.

- **CSCub05907**
  
  Symptoms: Reverse routes are not installed for an IPsec session while using dynamic crypto map.
  
  Conditions: This symptom occurs when the remote peer uses two or more IP addresses to connect and it goes down and comes back at least twice.
  
  Workaround: Issue “clear crypto session” for that peer.

- **CSCub10951**
  
  Symptoms: At RR, for an inter-cluster BE case, there are missing updates.
  
  Conditions: This symptom is observed with the following conditions:
  
  1. The following configuration exists at all RRs that are fully meshed:
     - `bgp additional-paths select best-external`
     - `nei x advertise best-external`
  
  2. For example, RR5 is the UUT. At UUT, there is,
     - Overall best path via RR1.
     - Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called “ic_path_rr5”.
     - Initially, RR5 advertises “ic_path_rr5” to its nonclient iBGP peers, that is, RR1 and RR3.
  
  3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
4. At PE6, reconfigure the route so that RR5 will have “ic_path_rr5” as its “best-external (internal) path”. At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

Workaround: Hard/soft clear.

- **CSCub28913**
  Symptoms: The Cisco ISR G2 with VPN-ISM drops packets over an IPsec tunnel-protected Tunnel interface.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T images, when there is a crypto map (static or dynamic) applied to the interface.
  Workaround:
  - Disable the ISM-VPN (issue “no crypto engine slot xx”, where xx is the slot number where the ISM is located).
  - Alternatively, change the configuration to use either static or dynamic VTIs for the tunnels where you need a crypto-map.

- **CSCub46570**
  Symptoms: The image cannot be built with an undefined symbol.
  Conditions: This symptom occurs as the commit error triggers the compiling issue.
  Workaround: There is no workaround.

- **CSCtq91063**
  Symptoms: A Cisco router may unexpectedly reload due to bus error or generate a spurious access.
  Conditions: This symptom occurs due to the F/S particle pool running out of free particles and the next packet failing to successfully obtain a particle. The F/S pool is used for fragmentation, so this will only occur when there is a large amount of fragmentation occurring. It has only been seen when there is a “ip mtu 1500” configured on a tunnel interface where the physical mtu is 1500 forcing packets to be fragmented on the physical interface rather than on the tunnel interface.
  Workaround 1: Remove “ip mtu 1500” from the tunnel interface.
  Workaround 2: Configure “service disable-ip-fast-frag”.
  Workaround 3: Reduce hold queue sizes such that the total size of the queues for all active interfaces in the system does not exceed 512.

- **CSCua21166**
  Symptoms: Unable to form IPSec tunnels due to the following error:
  “RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license.”
  Conditions: This symptom occurs when even though the router does not have 225 IPsec SA pairs, the error will prevent IPSec from forming. Existing IPSec SAs will not be affected.
  Workaround: Reboot to clear out the leaked counter, or install hsec9, which will disable CERM (Crypto Export Restrictions Manager).
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.8/2.3:
  No CVE ID has been assigned to this issue.
Additional information on Cisco’s security vulnerability policy can be found at the following URL:

- **CSCua60100**
  Symptoms: The router crashes at ip_acl_peruser_ctxt_free while clearing the calls.
  Conditions: The symptom is observed when an ACL filter is applied on the input direction and then the session is established. When you try to clear the session, the router crashes.
  Workaround: There is no workaround.

- **CSCua70065**
  Symptoms: CUBE reloads on testing DO-EO secure video call over CUBE when SDP passthru is enabled.
  Conditions: This symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.
  Workaround: There is no workaround.

- **CSCtz69084**
  Symptoms: The switch crashes when trying to enable IPsec MD5 authentication on the SVI.
  Conditions: This symptom is observed with the following conditions:
  
  ```
  VLAN 101
  SW1--------SW2
  
  1) Configure the IPsec MD5 authentication in global configuration mode.
  ipv6 router ospf 1
  area 0 authentication ipsec spi 1000 md5 123456ABCDEF123456ABCDEF123456AB
  
  2) Configure the IPsec MD5 authentication as below in the interface mode with MD5 key 7 and device crashes.
  ```
  Workaround: There is no workaround.

- **CSCua18166**
  Symptoms: When sub appid is triggered by end points, the network does not recognize it and displays it as “Unknown identifier”.
  Conditions: This symptom occurs when the limitation results in not supporting traffic classification based on sub appid.
  Workaround: There is no workaround.

- **CSCub47910**
  Symptoms: Unexpected reboot is seen due to Bus Error when using software version Cisco IOS Release 15.2(4)M1.
  Conditions: This symptom is observed when SSL VPN is configured on the Cisco ISR in Cisco IOS Release 12.5(4)M1, where the CEF process running in the context of SSL is being interrupted or asked for relinquishing of CPU.
  Workaround: There is no workaround.

- **CSCub91815**
  Symptoms: Certificate validation fails with a valid certificate.
  Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.
  Workaround: There is no known workaround.
• CSCuc07799
  Symptoms: The router crashes while booting with Cisco IOS Release 15.2(4)M weekly images.
  Conditions: This symptom occurs when the ISM-VPN Module is inserted in the router.
  Workaround: There is no workaround.

Resolved Bugs—Cisco IOS Release 15.2(3)T1

Cisco IOS Release 15.2(3)T1 is a rebuild release for Cisco IOS Release 15.2(3)T. The bugs in this section are resolved in Cisco IOS Release 15.2(3)T1 but may be open in previous Cisco IOS releases.

• CSCtq24557
  Symptoms: The router crashes after deleting multiple VRFs. This happens very rarely.
  Conditions: This symptom is observed in a large-scale scenario.
  Workaround: There is no workaround.

• CSCtq39602
  Symptoms: The DMVPN tunnel is down with IPSec configured. The show dmvpn command from the spoke shows that the state is IKE.
  Conditions: This symptom is observed after heavy traffic is pumped from the DMVPN hub to the spoke for some time, that is, from a few minutes to a couple of hours.
  Workaround: Configuring “crypto ipsec security-association lifetime kilobytes disable” to disable volume-based rekeying will reduce the problem.

• CSCtq95384
  Symptoms: Even after the removal of NSR configurations, BGP still holds memory.
  Conditions: This symptom is observed after the removal of NSR configurations.
  Workaround: There is no workaround.

• CSCtr36083
  Symptoms: IKE SAs are not cleared. Ping fails over the IPsec tunnel.
  Conditions: This symptom occurs when SAs are cleared by using the clear crypto session local address command.
  Workaround: There is no workaround.

• CSCtr87070
  Symptoms: Enabling login fails with the error “% Error in authentication”.
  Conditions: This symptom is observed with TACACS single-connection.
  Workaround: Remove TACACS single-connection.

• CSCts32708
  Symptoms: Similar to CSCth80642, the Cisco IOS SSLVPN router fails to accept new sessions. Users will not be able to load the WebVPN login page. If you enable debug SDPs, you may see the “Sev 4:sdps_get_pak_from_tcp(),line 1080:tcp_getpacket returned error 2, tcb=0x6A9EFFEC” error message.
  Conditions: This symptom is observed when the router remains reachable. Otherwise, (that is, you can ping the WebVPN IP) the SSL process is running and listening on the right port. The show tcp tcb and show tcp brief all numeric commands show connections stuck in the CLOSED and
CLOSEWAIT state. Clearing the TCP TCB sessions does not restore connectivity. Taking WebVPN in/out of service does not restore connectivity. Disabling WebVPN CEF and rebooting does not prevent the issue. Rebooting does resolve the issue temporarily.

Workaround 1: Reboot.

Workaround 2: If available for your platform, get the fix for CSCth80642 and disable WebVPN CEF (you should reboot or clear the TCB connections after disabling WebVPN CEF). This may prevent the problem.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1:

CVE ID CVE-2011-3286 has been assigned to document this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:

- CSCts72911
  
  Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the nonrestarting peer (RR, in this case).
  
  Conditions: This symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the nonrestarting router does not send back the corresponding VPN prefixes towards the restarted router.
  
  Workaround: There is no workaround.

- CSCts85459
  
  Symptoms: Upon a reload, the cellular interface will not negotiate if a crypto map is applied to it.
  
  Conditions: This symptom is observed on a Cisco 881 router that has a cellular interface which dials to get an IP address and also acts as the VPN gateway. When you reload the router, the cellular interface does not connect if a crypto map is applied and you will see that IPsec fails to initialize because you do not have an IP address.
  
  Workaround: This situation remains until you manually remove the crypto map from the cellular interface. Then, you will see the chat-script starting and the whole dialing procedure starts. Then, the cellular link is up with an IP address. Reapply the crypto map again and the tunnel works fine.

- CSCtt17762
  
  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.
  
  Conditions: This symptom is observed on an IP PIM multicast network.
  
  Workaround: There is no workaround.

- CSCtt26692
  
  Symptoms: The router crashes due to memory corruption. In the crashinfo you may see:

  $SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxxx data
  xxxxxxxx chunkmagic xxxxxxxx chunk_freemagic EF4321CD -
  Process= 'CCSIP_SPI_CONTROL', ipl= 0, pid= 374
  chunk_diagnose, code = 1
  chunk name is MallocLite

  Conditions: This symptom occurs when the router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.
Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

- **CSCt34790**
  Symptoms: Unexpected drops occur due to a large shaping burst.
  Conditions: This symptom occurs on high-speed interfaces with large shape values.
  Workaround: There is no workaround.

- **CSCt94440**
  Symptoms: The Cisco ASR 1000 series router RP may reload.
  Conditions: This symptom is observed when an etoken is in use and the `show crypto eli all` command is issued.
  Workaround: Avoid using the `show crypto eli all` command. However, you can use the `show crypto eli` command.

- **CSCtu11013**
  Symptoms: The router crashes when the SAF forwarder is enabled.
  Conditions: This symptom is observed when the SAF forwarder is enabled.
  Workaround: Disable the SAF forwarder.

- **CSCtu14409**
  Symptoms: The “Insufficient bandwidth 2015 kbps for bandwidth guarantee” error message is displayed when configuring a policy map with “priority level xxx” and then updating it with “police cir xxx”.
  Conditions: This symptom occurs when the priority is configured without a specific rate. This issue is only seen with a Cisco ASR 1000 series router.
  Workaround: Configure police before priority.

- **CSCtu22167**
  Symptoms: SP crashes.
  Conditions: This symptom is observed under the following conditions:
  - When unicast prefixes have local labels.
  - When the tunnel is the next-hop for those prefixes.
  - When the topology is modified (that is, when you remove or shut down the physical interface) so that the tunnel’s destination address is reachable via the tunnel.
  Workaround: Ensure that the tunnel endpoint peer does not advertise the prefixes to reach the tunnel endpoint.

- **CSCtu35116**
  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.
  Conditions: This symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.
  Workaround: There is no workaround.

- **CSCtu43120**
  Symptoms: Service accounting start is not sent for L2TP sessions.
Conditions: This symptom is observed with L2TP.
Workaround: There is no workaround.

- CSCtw61192
  Symptoms: When the **redistribute static** command has the **route-map** and the **set tag** arguments, and you enter the **no redistribute static** command, the router sends out only one query and the remaining routes get stuck in active state indefinitely.
  Conditions: This symptom is observed only when you set a tag to a redistributed route.
  Workaround: There is no known workaround.

- CSCtw61872
  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.
  Conditions: This symptom is observed when executing a complex sort with top-talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):

  ```text
  sh flow monitor QoS_Monitor cache sort highest counter packets top 1000
  sh flow monitor QoS_Monitor cache sort highest counter packets top 10000
  ```

  Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw62213
  Symptoms: When two Cisco 3945E routers are connected to each other and are performing IPSLA operations, the responder sees a drop in packets coinciding with license update process execution.
  Conditions: This symptom is observed when two Cisco 3945E routers are connected back to back while performing IPSLA UDP-jitter operation.
  Workaround: Increasing the input queue length on the interface and SPD queue length is a valid workaround.

- CSCtw62310
  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service-policy”.
  Conditions: This symptom is observed when removing the policy-map from map-class.
  Workaround: There is no workaround.
  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw68089
  Symptoms: The routing event detector is not present on Integrated Services Routers such as the Cisco 2800 series.
  Conditions: This symptom occurs for all releases on generation one Cisco ISR routers running Cisco IOS Release 15.2(2)T.
  Workaround: There is no workaround.

- CSCtw73530
  Symptoms: Unable to delete metadata sessions.
Conditions: This symptom is observed when more than 100 metadata sessions are created.
Workaround: Disable metadata and then enable it. Note that this will remove all the flows.

- CSCtw82120
  Symptoms: Cisco IOS might restart when the DMVPN QoS policy-map name is modified at the hub tunnel.
  Conditions: This symptom occurs when the DMVPN/QoS service-policy name is modified on the hub tunnel, and there are several spokes configured with the same NHRP group name. There could be a slim timing window during which Cisco IOS might get restarted due to a race-condition.
  Workaround: Waiting for some time before issuing the next command to change the QoS policy-map name would greatly minimize the chance to hit this race-condition.

- CSCtw86712
  Symptoms: RP crashes.
  Conditions: This symptom is observed when you apply certain tunnel configurations.
  Workaround: There is no workaround.

- CSCtw94598
  Symptoms: Web authentication does not work after an upgrade. NAS-Port-Type = Async.
  Conditions: This symptom is observed when you upgrade to Cisco IOS Release 12.2 (58)SE2 or later or to the Cisco IOS 15.0(1)SE train.
  Workaround: Change NAS-Port-Type on AAA Server to match the new value.

- CSCtw95189
  Symptoms: The “%Unknown DHCP problem. No allocation possible” error is observed in the DHCP error log.
  Conditions: This symptom occurs when open access is enabled and the supplicant is authz failed. Then, DHCP IP address assignment does not take place.
  Workaround: There is no workaround.

- CSCtw98456
  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.
  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).
  For example, the IVRF routing table should show:
  
  \[S \quad 10.0.0.0 \quad [1/0] \quad \text{via} \quad 192.168.0.1, \text{GigabitEthernet1/0/1}\]

  but instead it shows:
  
  \[S \quad 10.0.0.0 \quad [1/0] \quad \text{via} \quad 192.168.0.1\]

  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.
  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in \texttt{show crypto ipsec sa}) remain at zero.
Conditions: This symptom has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other Cisco IOS versions and other hardware platforms may be affected.

Workaround: Configure a static route to the remote network. For example:

```
ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- **CSCtx04709**

  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.

  Conditions: This symptom is observed when a multiple route goes down at the same time, and query arrives from neighbor router. Finally, neighbor detects SIA for affected router and neighbor state is flap. However, active entry is remaining after that, and route is not updated.

  Workaround: The `clear ip eigrp topology network mask` command may remove unexpected active entry.

- **CSCtx27813**

  Symptoms: The evaluation license cannot be used on a Cisco router.

  Conditions: This symptom is observed on a Cisco router when the evaluation license has high priority and the router is reloaded.

  Workaround: There is no workaround.

- **CSCtx29543**

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when issuing the `show ip route` command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exists.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when issuing the `show ip route` command or when the default route is updated.

  Workaround: There are two possible workarounds:

  1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then ensure that at least one supernet route for all possible mask lengths exists at all times, for example, by configuring summary routes that do not interfere with normal operation.

- **CSCtx31175**

  Symptoms: Framed-IP-Address is added twice in the PPP service-stop accounting record.

  Conditions: This symptom is observed with the following conditions:

  1. A user session exists on the Cisco ASR 1001 router.
  2. Stop one user’s session by using the `clear subscriber session username xxx` command on the Cisco ASR 1001 router.
3. The Cisco ASR 1001 router sends double “Framed-IP-Address” in service-stop accounting for one user’s session.

Workaround: Do not use the **clear subscriber session** command to clear the session. Instead, use the **clear pppoe** command.

- **CSCtx32329**

  Symptoms: When using the **show ipv6 rpf** command, the router crashes or displays garbage for RPF idb/nbr.

  Conditions: This symptom can occur when the RPF lookup terminates with a static multicast route that cannot be resolved.

  Workaround: Do not use static multicast routes, or make sure that the next hop specified can always be resolved. Do not use the **show** command.

- **CSCtx35064**

  Symptoms: Traffic remains on a blackholed path until the holddown timer expires for PfR monitored traffic class. Unreachables are seen on the path, but no reroute occurs until holddown expires.

  Conditions: This symptom is seen under the following conditions:

  - MC reroutes traffic-class out from a particular path (BR/external interface) due to the OOP condition on the primary path.

  - Shortly after enforcement occurs, an impairment on the new primary path occurs, causing a blackhole.

  - PfR MC does not declare OOP on the new primary path and attempts to find a new path until the holddown timer expires. This causes traffic loss.

  Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

- **CSCtx38806**

  Symptoms: SSL VPN users lose connectivity as soon as a Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

  This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

  The problem affects Firefox also (version 10.0.1), displaying the following message:

  “The page isn’t redirecting properly”

  Conditions: This symptom is observed on Cisco IOS that is acting as a headend for SSL VPN connections.

  Workaround: Any of the following workarounds will work:

  1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS.

  2. Uninstall the update.

  3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

     webvpn gateway gateway name
     ssl encryption rc4-md5

  4. Use AC 2.5.3046 or 3.0.3054.

  5. Use older versions of Firefox (9.0.1).
Further Problem Description: For AnyConnect users, the following user error message is seen:
“Connection attempt has failed due to server communication errors. Please retry the connection”
The AnyConnect event log will show the following error message snippet:
Function: ConnectIfc::connect Invoked
Function: ConnectIfc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for
PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.
If you believe that there is new information that would cause a change in the severity of this issue,
please contact psirt@cisco.com for another evaluation.
Additional information on Cisco’s security vulnerability policy can be found at the following URL:

- CSCtx45373
  Symptoms: Under `router eigrp virtual-name` and `address-family ipv6 autonomous-system 1`,
  when you enter `af-interface Ethernet0/0` to issue a command and exit, and later, under `router bgp 1` and
  `address-family ipv4 vrf red`, you issue the `redistribute ospf 1` command, the “VRF specified
does not match this router” error message is displayed. When you issue the `redistribute eigrp 1`
  command, it gets NVGENd without AS number.
  Conditions: This symptom occurs under `router eigrp virtual-name` and `address-family ipv6 autonomous-system 1`,
  when you enter `af-interface Ethernet0/0` to issue a command and exit, and later, under `router bgp 1` and
  `address-family ipv4 vrf red`, you issue the `redistribute ospf 1` command.
  Workaround: Instead of using the `exit-af-interface` command to exit, if you give a parent mode
  command to exit, the issue is not seen.

- CSCtx49098
  Symptoms: A crash occurs at `udb_pre_feature_unbind_cleanup`.
  Conditions: This symptom is observed when a complex 3 level HQoS policy is configured on the
  interface and it is manipulated with changes.
  Workaround: Do not manipulate the QoS policy while it is being used or avoid using the same child
  policy multiple times in the parent policy.

- CSCtx54882
  Symptoms: A Cisco router may crash due to Bus error crash at `voip_rtp_is_media_service_pak`.
  Conditions: This symptom has been observed on a Cisco router running Cisco IOS
  Release 15.1(4)M2
  Workaround: There is no known workaround.

- CSCtx55357
  Symptoms: Auto RP messages are permitted through “ip multicast boundary”.
  Conditions: This symptom is observed when the ACL associated with the multicast boundary
  matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.
  Workaround: Use “no ip pim autorp” to disable Auto RP completely from this device.

- CSCtx57073
  Symptoms: A Cisco router may crash with the following error: “Segmentation fault(11), Process =
  Metadata HA”
Conditions: This symptom is observed while upgrading the router from Cisco IOS XE Release 3.6 to mcp dev.
Workaround: The required changes have been made with this DDTS to prevent the crash.

- **CSCtx64347**
  Symptoms: Despite open access being configured on the port, traffic to/from the client is blocked.
  Conditions: This symptom occurs when an authenticating port with open-access and multi-auth hostmode configured, is interrupted.
  Workaround: There is no workaround.

- **CSCtx64684**
  Symptoms: While configuring the ISIS on two Cisco 2921 routers connected back to back, the ISIS neighbors do not come up.
  Conditions: This symptom is observed only on the SVI interface. This issue is only seen with EHWIC.
  Workaround: If the router has an L3 port, form a neighborship on a physical interface directly or create dot1q subinterfaces if peering is required on multiple VLANs.

- **CSCtx66030**
  Symptoms: A Cisco router handling SIP registrations/unregistrations may unexpectedly reload. This symptom is observed on the following devices:
    - SIP-CME
    - SIP-SRST GW
    - CUBE
  Conditions: This symptom is observed when the number of SIP registrations/unregistrations handled is more than 320.
  Workaround: Limit the number of registrations/unregistrations to less than 320.

- **CSCtx67474**
  Symptoms: An update message is sent with an empty NLRI when the message consists of a 2byte AS-path in ASPATH attribute and a 4byte value aggregate attribute.
  Conditions: This symptom occurs when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.
  Workaround: Move all the 2byte AS peers to a separate update-group using a nonimpacting outbound policy like “advertisement-interval”.

- **CSCtx68100**
  Symptoms: On a system having SP-RP, the reload reason is not displayed correctly. Once the system crashes, in all subsequent reloads the last reload reason is displayed as crash.
  Conditions: This symptom is observed on a system having SP-RP. The reload reason is shown wrongly when the `show version` CLI is executed.
  Workaround: There is no workaround.

- **CSCtx74342**
  Symptoms: After an interface goes down or is OIRed, in a routing table, you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next-hop interface set to the interface that is down.
Conditions: This symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 seconds default).

Workaround: Configuring the SPF throttle timer can change the interval.

Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Routershow ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
    B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
    IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
    ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
    1 - LISP
    O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O  2001::/64 [110/10]
    via Ethernet0/0, directly connected
```

- CSCx82775
  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.
  Conditions: This symptom is observed when MTP is invoked for calls.
  Workaround: Reload the router or perform a no sccp/sccp.

- CSCx86674
  Symptoms: ATM VPI/VCI does not come up after upgrading to Cisco IOS Release 15.1(4)M4.
  Conditions: This symptom is observed when upgrading to Cisco IOS Release 15.1(4)M4, which was an engineering build given for addressing CSCx09973.
  Workaround: ATM port shut/no shut resolves the issue. However, it refers to about 5000+ nodes here or “config dsl-group 0 pairs 0” instead of dsl-group auto under controller SHDSL.

- CSCx87646
  Symptoms: Firmware behavior options can only be used if “service internal” is activated.
  Conditions: The condition under which this symptom is observed is unknown.
  Workaround: There is no workaround.

- CSCx99544
  Symptoms: Exception occurs when using the no aaa accounting system default vrf VRF3 start-stop group RADIUS-SG-VRF3 command:

```
router(config)# no ip vrf VRF3
router(config)# no aaa accounting system default vrf VRF3 start-stop group
RADIUS-SG-VRF3

%Software-forced reload
```
  Conditions: This symptom is observed with the following conditions:
  - Hardware: Cisco ASR 1001 router.
• CSCty01234
Symptoms: A router running Cisco IOS may reload unexpectedly.
Conditions: This symptom is observed only with low-end platforms using VDSL interfaces, such as a Cisco 887 router. It also requires that the `qos pre-classify` command be used in conjunction with IPsec and GRE, such as in a DMVPN configuration.
Workaround: Do not use the `qos pre-classify` command.

• CSCty02403
Symptoms: An EIGRP topology entry with bogus next-hop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus next-hop. So if you have a default route received from some neighbors, then that default route will also flap.
Conditions: It can only occur when more then one attribute set in any route received from a neighbor.
Workaround: Do not set more then one attribute in the route.

• CSCty03629
Symptoms: Traffic from a client with a valid IP-SGT mapping is dropped by the firewall.
Conditions: This symptom occurs when NAT is colocated with SGFW1.
Workaround: There is no workaround.

• CSCty03745
Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.
Conditions: This symptom occurs when the IPv4 default route exists, that is:

```
ip route 0.0.0.0 0.0.0.0 <next-hop>
```
Or a certain static/IGP route exists. For example:

```
ip route 0.0.253.0 255.255.255.0 <next-hop>
```
Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family.
For example, router bgp 65000 address-family l2vpn vpls neighbor 10.10.10.10 next-hop-self
Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

• CSCty05092
Symptoms: EIGRP advertises the connected route of an interface which is shut down.
Conditions: This symptom is observed under the following conditions:
1. Configure EIGRP on an interface.
2. Configure an IP address with a supernet mask on the above interface.
3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.
Workaround 1: Remove and add INTERFACE VLAN xx.
Workaround 2: Clear ip eigrp topology x.x.x.x/y.
• CSCty05150
Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.
Conditions: This symptom occurs when the stub ABR is configured in a VRF without “capability vrf-lite” configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.
Workaround: Remove and reconfigure “area x stub”.

• CSCty12083
Symptoms: A Cisco 819 router with the C819HG+7 SKU reloads.
Conditions: This symptom is observed on a Cisco 819 router with the C819HG+7 SKU reloads while running Cisco IOS Release 15.1(4)M3.8.
Workaround: There is no workaround.

• CSCty15615
Symptoms: The policy in direction A may disappear after removing the policy from direction B. The policies no longer show up under the interface in `sh policy-map int` or `show running`.
Conditions: This symptom is observed with policies on both input and output directions, and when you remove the policy from one of the directions. This issue is seen on Cisco 7200/7600 platforms.
Workaround: There is no workaround.

• CSCty22840
Symptoms: A router can crash due to a Watchdog timeout on the NTP process as it fails to unpeer from an NTP peer that had already been removed. In addition, the following error might be seen in the system log:

```plaintext
NTP Core (ERROR): peer struct for X.X.X.X not in association table
```
Conditions: This symptom is observed when active changes occur in NTP, that is, new peers or servers are added at boot time as part of the existing configuration or during normal operation as part of a new configuration.
Workaround: Configure NTP to use the ACL with the `ntp access-group peer` command to explicitly define which hosts can function as an NTP peer.

• CSCty24606
Symptoms: Under certain circumstances, the Cisco ASR 1000 series router’s ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.
Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs can not be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.
Workaround: There is no workaround.

• CSCty24707
Symptoms: Standby RP continually reboots and never recovers.
Conditions: This symptom is observed during an RP standby switchover with QoS applied to ISG sessions.
Workaround: Shut down the virtual template interface and do a switchover.
• CSCty25810
  Symptoms: Tracebacks are observed on the PAN module in auth_feature_critical_get_authorized_domain_any() / dot1x_matm_mac_addr_learned() functions.
  Conditions: This symptom occurs due to an invalid HWIDB pointer. HWIDB is NULL for the mac-addresses learned over the CPU_PORT in case of L2VPN.
  Workaround: There is no workaround.
• CSCty30886
  Symptoms: A standby RP reloads.
  Conditions: This symptom is observed when bringing up PPPoE sessions with configured invalid local IP address pool under the virtual-template profile and “aaa authorization network default group radius” on the box with no radius present. No IP address is assigned to the PPPoE Client.
  Workaround: There is no workaround.
• CSCty37020
  Symptoms: Learned inside BGP prefixes are not getting added into the MC database.
  Conditions: This symptom is observed with learned inside BGP prefixes.
  Workaround: There is no workaround.
• CSCty37445
  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.
  Conditions: This symptom is observed when on the spoke you have a distribute list route-map command setting tags.
  Workaround: Once you remove that command EIGRP works normally.
• CSCty42626
  Symptoms: Certificate enrollment fails for the Cisco 3945 router and the Cisco 3945E router due to digital signature failure.
  Conditions: This symptom is observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.
  Workaround: There is no workaround.
• CSCty43587
  Symptoms: A crash is observed with memory corruption similar to the following:
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX, dealloc XXXXXXXX
  Conditions: This symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.
  Workaround: There is no workaround.
• CSCty46273
  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) may crash when the connected routes in the RIB flap.
  Conditions: This symptom is observed when LISP tracks the reachability of routing locators (RLOCs) in the RIB. For the crash to occur, a locator being watched by LISP must be covered by a route that is itself covered by a connected route. If both these routes are removed from the RIB in close succession, there is a small possibility that the race-condition resulting in this crash may be hit.
Bugs for Cisco IOS Release 15.2(3)T

OL-25471-04 Rev. P0

Workaround: There is no workaround.

- CSCty49656
  Symptoms: A crash is observed when executing the \textbf{no ip routing} command.
  Conditions: This symptom is observed under the following conditions:
  1. Use a Cisco IOS image that has fix for CSCtg94470.
  2. Configure OSPF.
  3. Enable multicast.
  4. Create several (>6000) routes in the network to be learned by OSPF.
  5. Wait for OSPF to learn all the (>6000) routes from the network.
  Finally, executing the \textbf{no ip routing} command may crash the box.
  Workaround: There is no workaround.

- CSCty53243
  Symptoms: Video call fails in the latest mcp_dev image
  asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has
  the ucinfra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous
  mcp_dev image
  asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.
  Conditions: This symptom is observed when CUBE changes the video port to “0” in 200 OK sent to
  the UAC.
  Workaround: There is no workaround.

- CSCty54434
  Symptoms: ISRG2 with ISM VPN is not bringing up more than one tunnel in a crypto map-based
  scenario with large certificates (4096 bit).
  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T and Cisco IOS
  Release 15.2(2)T.
  Workaround: Configure IKEv2 fragmentation so that the fragmentation/reassembly is handled by
  IKE code rather than by IPsec.

- CSCty58992
  Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.
  Conditions: This symptom is observed under the following conditions:
  - Cluster is in v6 mode.
  - A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3(SIP POTS),
    which is when the issue occurs.
  Workaround: There is no workaround.

- CSCty61212
  Symptoms: The removal of crypto map hangs the router.
  Conditions: This symptom is observed with the removal of GDOI crypto map from interface.
  Workaround: There is no workaround.

- CSCty65334
  Symptoms: Unconfigured crypto ACL causes the Cisco 3900 router to crash.
Conditions: This symptom is observed with a Cisco 3900 image with ISM crypto engine installed and enabled. This may also affect the Cisco 2900 and Cisco 1900 routers with ISM crypto engine installed and enabled.

Workaround: When changing the crypto ACL configuration, disable the ISM crypto engine first using the `no crypto engine slot 0` command, and then change the ACL. After changing the ACL, reload the router with ISM enabled.

- **CSCty68348**

  Symptoms: If the OSPF v2 process is configured with the `nsr` command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:
  - The OSPF router is configured for “nsr”.
  - Shutdown/no shutdown of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- **CSCty68402**

  Symptoms: NTT model 4 configurations are not taking effect.

  Conditions: This symptom occurs under the following conditions:

  ```
  policy-map sub-interface-account
  class prec1
  police cir 4000000 conform-action transmit exceed-action drop
  account
  class prec2
  police cir 3500000 conform-action transmit exceed-action drop
  account
  class prec3
  account
  class class-default fragment prec4
  bandwidth remaining ratio 1
  account
  
  policy-map main-interface
  class prec1
  priority level 1
  queue-limit 86 packets
  class prec2
  priority level 2
  queue-limit 78 packets
  class prec3
  bandwidth remaining ratio 1
  random-detect
  queue-limit 70 packets
  class prec4 service-fragment prec4
  shape average 200000
  bandwidth remaining ratio 1
  queue-limit 62 packets
  class class-default
  queue-limit 80 packets
  ```

  Workaround: There is no workaround.
• CSCty73817

Symptoms: In large-scale PPPoE sessions with QoS, the Standby RP might reboot continuously (until the workaround is applied) after switchover. This issue is seen when the QoS Policy Accounting feature is used. When the issue occurs, the Active RP remains operational and the Standby RP reboots with the following message:

%PLATFORM-6-EVENT_LOG: 43 3145575308: *Mar 16 13:47:23.482: %QOS-6-RELOAD: Index addition failed, reloading self

Conditions: This symptom occurs when all the following conditions are met:

1. There is a large amount of sessions.
2. The QoS Policy Accounting feature is used.
3. Switchover is done.

Workaround: Bring down sessions before switchover. For example, shut down the physical interfaces that the sessions go through, or issue the Cisco IOS command clear pppoe all.

• CSCty76106

Symptoms: A crash is seen after two days of soaking with traffic.

Conditions: This symptom occurs with a node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes, and bidirectional traffic.

Workaround: There is no workaround.

• CSCty77190

Symptoms: DTLS is switched back to TLS after reconnect.

Conditions: This symptom is observed with the following conditions:

- Test image c3845-advsecurityk9-mz.152-2.T1.InternalUseOnly
- Test version - Cisco IOS Release 15.2(01)T

Workaround: Restart the AnyConnect client.

• CSCty78435

Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

• CSCty84989

Symptoms: IKEv2 pushed routes are not installed in the IPv6 inner VRF routing table.

Conditions: This symptom occurs when using IKEv2 on pure IPv6 tunnels with tunnel protection IPsec and a VRF on the tunnel.

Workaround: There is no workaround.
• CSCty85634
  Symptoms: A router configured with the Locator ID Separation Protocol (LISP) without an EID-table for the default VRF fails to maintain its LISP map-cache during an RP switchover. After the switchover, the existing remote EID entries in CEF eventually expire and new data packet signals result in repopulation of the LISP map-cache, thus resuming normal operation.
  Conditions: This symptom occurs in a LISP configuration that contains EID-tables for VRFs other than the default and does not contain an EID-table for the default VRF.
  Workaround: Configure an EID-table for the default VRF before the switchover with some LISP configuration such as “ipv4 itr”.

• CSCty86111
  Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.
  Conditions: This symptom is observed with Cisco ISR G2 router.
  Workaround: There is no workaround.

• CSCty94289
  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.
  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.
  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

• CSCty97784
  Symptoms: The router crashes.
  Conditions: This symptom is observed when NBAR is enabled, that is, “match protocol” actions in the QoS configuration, or “ip nbar protocol-discovery” on an interface or NAT is enabled and “ip nat service nbar” has not been disabled.
  Workaround: There is no workaround.

• CSCty98834
  Symptoms: The Cisco c2900, c3900, and c1900 IOS with the ISM VPN crypto engine might crash after some time when you run out of memory on the ISM VPN engine as there are memory leaks during rekey.
  Conditions: This symptom occurs when the ISM VPN crypto engine is enabled.
  Workaround: Disable the ISM VPN module using the no crypto engine slot 0 command.

• CSCtz08037
  Symptoms: The router fails to pass any traffic after receiving the “%OCE-3-OCE_FWD_STATE_HANDLE: Limit of oce forward state handle allocation reached; maximum allowable number is 50000” error message.
  Conditions: This symptom is observed MPLS L2VPN is configured with EoMPLSoGRE with IPSec encryption on top of the VTI tunnel with IPSec encryption (double encryption).
  Workaround: Reload the router.

• CSCtz15211
  Symptoms: The ISM card does not encrypt packets through a double encrypted tunnel.
Conditions: This symptom is observed with ISR g2 with the ISM module and crypto configured for GRE over IPsec packets to be encrypted through a VTI (double encryption).
Workaround: Use onboard encryption.

- **CSCtz24280**
  Symptoms: MSP flows are not identified.
  Conditions: This symptom is observed when “proxy-call-id” is present in the “Route” header of SIP packets.
  Workaround: Remove proxy servers from the topology.

- **CSCtz25364**
  Symptoms: GM to GM communication between ISM VPN and the Cisco ASR 1000 series router with TBAR enabled is broken.
  Conditions: This symptom occurs when ISM VPN and the Cisco ASR 1000 series router are GMs and TBAR is enabled.
  Workaround: Disable ISM VPN or disable TBAR and switch to counter-based anti-replay.

- **CSCtz27137**
  Symptoms: An upgrade to the S640 signature package may cause a Cisco IOS router to crash.
  Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:
  - Cisco IOS Release 12.4(24)T4
  - Cisco IOS Release 15.0(1)M4
  - Cisco IOS Release 15.0(1)M8
  - Cisco IOS Release 15.2(3)T
  Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:
  - Access the router via the console.
  - Enter break sequence to access ROMmon mode.
  - Change the config-register value to 0x2412.
  - Boot the router to bypass the startup-configuration.
  - Configure the basic IP parameters.
  - TFTP a modified configuration to the router’s running-configuration with Cisco IOS IPS disabled.
  - Reset the config-register to 0x2102.
  - Enter the `write memory` command and reload.

- **CSCtz59429**
  Symptoms: Packets do not match a flow with the attribute “application category voice-video”.
  Conditions: This symptom occurs when a flow with the attribute “application category voice-video” is matched for the same attribute.
  Workaround: There is no workaround.
• CSCtz70938
  Symptoms: When the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.
  Conditions: This symptom occurs when the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.
  Workaround: Do not use boot configuration files other than startup-configuration when there are “service-module” CLI in the configuration.

• CSCtz72390
  Symptoms: The name mangling functionality is broken. Authorization fails with the “IKEv2:AAA group author request failed” debug message.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.
  Workaround: There is no workaround.

• CSCtz85134
  Symptoms: A manually generated self-signed trustpoint gets erased and a new trustpoint is autogenerated when SSL-Express Accelerator is enabled and the router’s configuration is saved and it is reloaded.
  Conditions: This symptom is observed when the trustpoint is generated manually and SSL-Express Accelerator must be enabled. This issue is seen only when the configuration is saved and the router is reloaded.
  Workaround: Disable SSL-Express Accelerator.

• CSCtz99916
  Symptoms: The Cisco 3945 router does not respond to a reinvite from CVP.
  Conditions: This symptom occurs when call legs are not handled in a proper IWF container.
  Workaround: There is no workaround.

• CSCua22313
  Symptoms: SSLv3.0- and TLSv1.0-based data transfer using certain older client applications (like IE6) fails.
  Conditions: This symptom is observed when the HTTPS page is fetched by a client application that does not have a fix for the BEAST vulnerability (http://blogs.cisco.com/security/beat-the-beast-with-tls/) and the connection is optimized by SSL-Express Accelerator in WAAS-Express.
  Workaround: Upgrade the client application to the latest version or at least a version that has a fix for BEAST in case of Internet Explorer version 8 or higher.

• CSCua08883
  Symptoms: Tracebacks are seen in the Persaqos script.
  Conditions: This symptom is observed with the Persaqos script.
  Workaround: There is no workaround.

• CSCtz93002
  Symptoms: 117 images fail with the following error message:

  `make-3.79.1-p7[3]: ***`
Bugs

[crypto/sub_subsys_crypto_ipsec_common.o/crypto_classify.o] Error 1
make-3.79.1-p7[2]: [CBSCONTEXT-obj-4k] Error 2 (ignored)

Conditions: This symptom is observed with an automatic merge.
Workaround: There is no workaround.

Open Bugs—Cisco IOS Release 15.2(3)T

All the bugs listed in this section are open in Cisco IOS Release 15.2(3)T. This section describes only severity 1, severity 2, and select severity 3 bugs.

- **CSCtx31294**
  Symptoms: Anyconnect is unable to connect to the Cisco IOS headend (ISR-G2) when cert-based authentication is in use.
  Conditions: This symptom is observed with the following conditions:
  1. Cert-based authentication is configured using “authentication local rsa-sig” on the Cisco IOS headend.
  2. Remote authentication on the Cisco IOS headend can be EAP or rsa-sig. The Anyconnect client is unable to connect, and hence the tunnel is not established.
  Workaround: There is no workaround.

- **CSCty53243**
  Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.
  Conditions: This symptom is observed when CUBE changes the video port to “0” in 200 OK sent to the UAC.
  Workaround: There is no workaround.

- **CSCty57085**
  Symptoms: When accessing the Sharepoint present at HQ and downloading a file of 8.5 MB, the transaction time is more when compared to no WAAS.
  Conditions: This symptom is observed when there is a large amount of traffic.
  Workaround: There is no workaround.

- **CSCty80566**
  Symptoms: Cisco IOS crashes.
  Conditions: This symptom is observed with Cisco IOS during normal usage.
  Workaround: There is no workaround.

- **CSCty90223**
  Symptoms: A crash occurs at nhrp_nhs_recover_co_destroy during setup and configuration.
  Conditions: This symptom is observed under the following conditions:
  1. Add and remove the ip nhrp configuration over the tunnel interface on the spoke multiple times.
  2. Do shut/no shut on the tunnel interface.
3. Rapidly change IPv6 addresses over the tunnel interface on the spoke side and on the hub side multiple times.
4. Replace the original (correct) IPv6 addresses on both the spoke and the hub.
5. 5) Wait for the registration timer to start.

The crash, while not consistently observed, is seen fairly often with the same steps.

Workaround: There is no known workaround.

**Resolved Bugs—Cisco IOS Release 15.2(3)T**

All the bugs listed in this section are resolved in Cisco IOS Release 15.2(3)T. This section describes only severity 1, severity 2, and select severity 3 bugs.

- **CSCtj48387**
  Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP related errors.
  Conditions: This symptom occurs when DHCP enabled and sessions get DHCP information from a RADIUS server.
  Workaround: There is no workaround.

- **CSCtq64987**
  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.

  An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

- **CSCtr46123**
  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

- **CSCtr91106**
  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.
Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts38429

The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

- CSCtt16051

Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

- CSCtt19027

Symptoms: When ACL is applied to the serial interface or Gigabit interface, ping failure seen even though the permit statement is there.

Conditions: The symptom is observed when ACL is configured on the serial interface or Gigabit interface.

Workaround: Enable EPM by installing the security license.

Further Problem Description: This is seen with those images where EPM is not supported and because of that an EPM call always gives a return value as “deny” due to registry call.

- CSCtt35379

Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp
CSCtt45381
Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.
Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

CSCtu57226
Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.
Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

CSCtw73530
Symptoms: Unable to delete metadata sessions.
Conditions: This symptom is observed when more than 100 metadata sessions are created.
Workaround: Disable metadata and then enable it. Note that this will remove all the flows.

CSCtw99591
Symptoms: cpfrMCIndex OID loops and does not increase.
Conditions: This symptom is observed while doing a MIB walk.
Workaround: Poll individual MIBs or walk around the PfR MIB.

CSCtx04712
Symptoms: Removal of crypto map hangs the router.
Conditions: The symptom is observed following removal of “gdoi crypto map” from interface.
Workaround: There is no workaround.

CSCtx06801
Symptoms: Certain websites may not load when content-scan is enabled. Delays of up to a few seconds may be seen.
Conditions: The symptom is observed when content-scan is enabled.
Workaround: Though not always, refreshing the page sometimes helps.

Further Problem Description: The problem is due to GET request being segmented. For example, a huge get request of 1550 may come from the client in two different packets such as 1460+90=1550.

- **CSCtx40818**
  - Symptoms: Traffic drops in a Cisco and displays the following error message:

    ```
    %IP-3-LOOPPAK: Looping packet detected and dropped -
    src=122.0.0.11, dst=121.0.0.11, hl=20, tl=40, prot=6, sport=80, dport=57894
    ```

    Conditions: This symptom is observed if the WAAS, NAT and firewall are enabled.
    Workaround: Disable WAAS.

- **CSCtx47493**
  - Symptoms: NTLM authentication does not work.
  - Conditions: The symptom is observed when **ip admission ntlm rule** is configured on the interface.
  - Workaround: There is no workaround.

- **CSCtx56174**
  - Symptoms: Cisco router hangs until a manual power cycle is done. If the scheduler **isr-watchdog** command is configured, the device will crash and recover instead of hanging until a power cycle is done.
  - Conditions: This is seen with websense URL filtering enabled and with zone based firewalls.
  - Workaround: Disable URL-based filtering.

- **CSCtx62790**
  - Symptoms: MSP chunks may increase causing memory depletion within 2 hrs of stress testing.
  - Conditions: This symptom is observed due to a corner negative scenario. Here, MSP gets separated from the IXIA client. A “NO RTSP PLAY” error message displays which completes the call or causes session teardown. This symptom is observed even with other protocols having immature call states.
  - Workaround: There is no workaround.

- **CSCtx64210**
  - Symptoms: An unprotected debug message prints out on the console.
  - Conditions: This symptom is observed during normal operation.
  - Workaround: There is no workaround.

- **CSCtx66011**
  - A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.
  - The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).
Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.

In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.

Only IKEv1 is affected by this vulnerability.

An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.

Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ike

Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication. Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- **CSCtx67290**
  
  **Symptoms:** A Cisco Session Border Controller crashes when receiving an oversize rtcp-fb element in the SDP.
  
  **Conditions:** The symptom is observed when there is an oversize rtcp-fb element in the SDP.
  
  **Workaround:** There is no workaround.

- **CSCtx87939**
  
  **Symptoms:** When the Mediatrace Poll command is invoked using WSMA interface, the “hops response received notifications” message is displayed. This message corrupts the WSMA output for the command.
  
  **Conditions:** This symptom is observed when Mediatrace poll is used in a WSMA interface.
  
  **Workaround:** There is no workaround.

- **CSCtx88093**
  
  **Symptoms:** A dialer idle timeout is not initiated after the watched route is installed back in the routing table while using a dialer watch list, causing the watch disconnect timer to not start.
  
  **Conditions:** This symptom occurs while using the `dialer-list x protocol ip deny` command to define interesting/uninteresting traffic and while there is traffic flowing over the dialer interface.
  
  **Workaround:** Use the following method to define interesting traffic instead of `dialer-list x protocol ip deny`:

  ```
  access-list x protocol ip deny dialer-list 1 protocol ip list x
  ```

- **CSCtx90299**
  
  **Symptoms:** The DMVPN IPsec sessions might get torn down and unable to re-establish themselves after experiencing link-flap events.
Conditions: In a scaled DMVPN environment, when physical-port link-state up/down events happen, there will be stormed IPSec events to tear down and/or re-negotiate the sessions; it might run into a bad state that it cannot establish new sessions. Hence, when those active sessions expire (by time period or volume based), it can no longer be re-created. After some period of time, no more active session remains on the router.

Workaround: Reload the router.

- **CSCtx92665**
  
  Symptoms: Executing the `show mediattrace session stat` command causes a crash at `__be_sla_mt_route_data_print`.
  
  Conditions: This symptom is observed when `show mediattrace session stat` or `show mediattrace session data` is used.
  
  Workaround: There is no workaround.

- **CSCty04384**
  
  Symptoms: IMA-DSLAPP crashes when doing interoperability testing with third-party DSLAMs.
  
  Conditions: Change line rates on CO sides with various loop lengths.
  
  Workaround: There is no workaround.

- **CSCty07771**
  
  Symptoms: CSCts55654 may cause extensive performance degradation.
  
  Conditions: This symptom is observed when normal QoS policy is applied on egress direction.
  
  Workaround: There is no workaround.

- **CSCty13747**
  
  Symptoms: Cisco Network Based Application Recognition (NBAR) applications with “engine-id=13” not shown or exported.
  
  Conditions: This symptom is observed while executing the `show flow exporter option application table` command.
  
  Workaround: The issue has been fixed.

- **CSCty54728**
  
  Symptoms: The `media-proxy {rsvp | metadata} <name>` command and its subcommands are not applied when a Cisco router reloads.
  
  Conditions: This symptom is observed when the `media-proxy {rsvp | metadata} <name>` command does not generate correct `show running-config` output.
  
  Workaround: Reload the router, and then configure the `media-proxy {rsvp | metadata} <name>` command and its subcommands.

- **CSCty58300**
  
  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.
  
  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.
  
  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.
Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-bgp
Caveats for Cisco IOS Release 15.2(2)T

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- **Symptoms**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

---

**Note**

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl). (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

- Resolved Caveats—Cisco IOS Release 15.2(2)T4, page 338
- Resolved Caveats—Cisco IOS Release 15.2(2)T3, page 345
- Resolved Caveats—Cisco IOS Release 15.2(2)T2, page 357
- Resolved Caveats—Cisco IOS Release 15.2(2)T1, page 378
- Open Caveats—Cisco IOS Release 15.2(2)T, page 394
- Resolved Caveats—Cisco IOS Release 15.2(2)T, page 398
Caveats for Cisco IOS Release 15.2(2)T

Resolved Caveats—Cisco IOS Release 15.2(2)T4

Cisco IOS Release 15.2(2)T4 is a rebuild release for Cisco IOS Release 15.2(2)T. The caveats in this section are resolved in Cisco IOS Release 15.2(2)T4 but may be open in previous Cisco IOS releases.

- **CSCts03251**
  Symptoms: A Cisco 2921 router running Cisco IOS Release 15.1(4)M with the “logging persistent” feature configured may crash.
  Conditions: This symptom is observed with the “logging persistent” feature.
  Workaround: Disable the “logging persistent” feature.

- **CSCts60458**
  Symptoms: There is a memory leak in PfR MIB.
  Conditions: This symptom occurs when PfR is configured.
  Workaround: There is no workaround.

- **CSCtw52610**
  Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.
  Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.
  Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure “max-xmit-utilization percentage 100”.

- **CSCtw78539**
  Symptoms: A Cisco ISR router running Cisco IOS Release 15.2(2)T may lose the ability to forward traffic via its Gigabit Ethernet interface due to a stuck Tx ring.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T1, 15.2(2)T, and 15.2(4)M. This is a regression issue that does not affect 15.0(1)M3 nor 15.1(4)M2 based on anecdotal accounts.
  During the event the following logs can be seen which indicate a spurious memory access has occurred:
  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0xXXXXXXXX reading 0x0
  %ALIGN-3-TRACE: -Traceback= 0xXXXXXXXX ...
  ```
  At this time, the Tx ring of the interface becomes hung, causing packet drops to accumulate at the output queue (as seen via “show interface”), effectively preventing traffic flow. For example:
  ```
  Total output drops: 25185 Output queue: 331/1000/25184 (size/max total/drops)
  ```
  Workaround: Reload the router or bounce the interface via “shut/no shut”.

- **CSCua05196**
  Symptoms: After the reload command is entered, the router gets crashed.
  Conditions: This symptom occurs when SSH traffic is sent.
  Workaround: Enable the warm reboot command.

- **CSCua15292**
  Symptoms: Router may crash unexpectedly with crypto in running-configuration.
  Conditions: The symptom is observed with a router running at normal operation. When it crashes, the error message below is found in the crashinfo file:
%CRYPTO-4-RECV_CRYPT_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=172.8.9.8, prot=50, spi=0xE8FB045F(3908746767), srcaddr=10.0.100.1, input
interface=GigabitEthernet0/0

Workaround: There is no workaround.

- **CSCua55785**
  Symptoms: Build breakage due to fix of CSCtx34823.
  Conditions: This issue occurs with CSCtx34823 fix.
  Workaround: CSCtx34823 change may be unpatched from the code-base.

- **CSCua73191**
  Symptoms: Anyconnect fails to work with IOS SSL VPN and reports the following message:
  The AnyConnect package on the secure gateway could not be located. You may be
  experiencing connectivity issues. Please try connecting again.

  Conditions: The issue was seen after upgrading to Cisco IOS Release 15.2(3)T.
  Workaround: Connecting via the portal might help.

- **CSCua75069**
  Symptoms: BGP sometimes fails to send an update or a withdraw to an iBGP peer (missing update)
  Conditions: This symptom is observed only when all of the following conditions are met:
  1. BGP advertise-best-external is configured, or diverse-path is configured for at least one
     neighbor.
  2. The router has one more BGP peers.
  3. The router receives an update from a peer, which changes an attribute on the backup path/repair
     path in a way which does not cause that path to become the best path.
  4. The best path for the net in step 3 does not get updated.
  5. At least one of the following occurs:
     - A subsequent configuration change would cause the net to be advertised or withdrawn.
     - Dampening would cause the net to be withdrawn.
     - SOO policy would cause the net to be withdrawn.
     - Split Horizon or Loop Detection would cause the net to be withdrawn.
     - IPv4 AF-based filtering would cause the net to be withdrawn.
     - ORF-based filtering would cause the net to be withdrawn.
     - The net would be withdrawn because it is no longer in the RIB.

  The following Cisco IOS releases are known to be impacted if they do not include this fix:
  - Cisco IOS Release 15.2T and later releases
  - Cisco IOS Release 15.1S and later releases
  - Cisco IOS Release 15.2M and later releases
  - Cisco IOS Release 15.0EX and later releases

  Older releases on these trains are not impacted.
  Workaround: If this issue is triggered by a configuration change, you can subsequently issue the
  **clear ip bgp neighbor soft out** command.
CSCua96354
Symptoms: Reload may occur when issuing the show oer and show pfr commands.
Conditions: This symptom is observed with the following commands:
   a. show oer master traffic-class performance
   b. show pfr master traffic-class performance
Workaround: There is no workaround.

CSCub67465
A vulnerability in the T1/E1 driver queue implementation of Cisco IOS Software could allow an unauthenticated, remote attacker to cause an interface wedge condition, which could lead to loss of connectivity, loss of routing protocol adjacency, and could result in a denial of service (DoS) scenario.
The vulnerability is due to incorrect implementation of the T1/E1 driver queue. An attacker could exploit this vulnerability by sending bursty traffic through the affected interface driver. Repeated exploitation could cause a DoS condition.
Workarounds to mitigate this vulnerability are available.
Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-wedge
Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.
Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

CSCub90459
Symptoms: If CUBE has midcall reinvite consumption enabled, it also consumes SIP 4XX responses. This behavior can lead to dropped or hung calls.
Conditions: This symptom occurs when midcall reinvite consumption is enabled.
Workaround: There is no workaround.

CSCuc55634
Symptoms: IPv6 static route cannot resolve the destination.
Conditions: This symptom is observed only when all of the following conditions are met:
1. A VRF is configured by the old style CLI (for example “ip vrf RED”).
2. Configure ip vrf forwarding RED under an interface.
3. Configure IPv6 address under the same interface (for example 2001:192:44:1::2/64)
5. Then, we are not able to ping the 2001:192:14:1::2 although we can reach 2001:192:44:1::1.
Workaround: There is no workaround.
- **CSCuc98021**  
  Symptoms: One-way voice audio issue is seen over CUBE after session reinvite is sent.  
  Conditions: This symptom is observed with the following call flows:  
  Signaling: Cisco IP phone ==> CUCM ==> CUBE ==> CCIPL ==> CCIPL IP phone  
  Media: Cisco IP phone <=== sRTP ==> CUBE <== RTP ==> CCIPL IP phone  
  Workaround: Do not use SRTP on the CUCM <-> CUBE leg.

- **CSCud01502**  
  Symptoms: A crash occurs in CME while accessing a stream in “sipSPIDtmfRelaySipNotifyConfigd”.  
  Conditions: This symptom occurs in CME.  
  Workaround: There is no workaround.

- **CSCud03273**  
  Symptoms: All the paths using certain next-hops under the route-map are marked inaccessible.  
  Conditions: This symptom occurs under the following conditions:  
  1. Configure peer groups.  
  2. Apply BGP NHT with route-map (no BGP neighbors are created or added to peer groups).  
  3. Configure the Prefix-list.  
  4. Configure the route-map.  
  5. Configure the BGP neighbor and add them to peer groups.  
  Workaround: Configure “route-map permit <seq-num> <name>” or activate at least one neighbor in “address-family ipv4”.

- **CSCud06887**  
  Symptoms: There is no sync of SADB on an active router when it reloads from the current standby router.  
  Conditions: This symptom occurs when the active and standby routers are up. Whenever a session is up, there is a sync of SADB from active to standby. When active reloads and is up, there is no sync of SADB from the current active router.  
  Workaround: Remove the isakmp-profile configuration under the crypto map.

- **CSCud22222**  
  Symptoms: On a router running two ISIS levels and fast-reroute, the router may crash if “metric-style wide level-x” is configured for only one level.  
  Conditions: Issue may happen if metric-style wide is configured for only one level on router running both levels, and fast-reroute is configured.  
  Workaround: Configure metric-style wide for both levels (by default).

- **CSCud41058**  
  Symptoms: There is a route-map which matches tags and set a new value. This route-map is used in an EIGRP outbound distribute list. One in 10 times based on the received route tag, the correct route tag value is not set while advertising out.  
  Conditions: The symptom is observed when you use a route map which matches tags and sets a new tag. Used in **distribute-list route-map name out**.  
  Workaround: Clear the EIGRP process or re-advertise the route.
• CSCud62864
Symptoms: When the Mid-call Re-INVITE consumption feature is active, CUBE consumes Re-INVITE which should change the media state from “sendonly” to “sendrcv”. This results in a one way or no way audio on the call.
Conditions: This symptom occurs when the CUBE Mid-call Re-INVITE consumption feature is enabled.
Workaround: There is no workaround.

• CSCud64812
A vulnerability in the implementation of the virtual fragmentation reassembly (VFR) feature for IP version 6 (IPv6) in Cisco IOS Software could allow an unauthenticated, remote attacker to cause an affected device to hang or reload, resulting in a denial of service (DoS) condition.
The vulnerability is due to a race condition while accessing the reassembly queue for IPv6 fragments. An attacker could exploit this vulnerability by sending a crafted stream of valid IPv6 fragments. Repeated exploitation may result in a sustained DoS condition.
Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability.
This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ipv6-vfr
Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.
Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

• CSCud67779
Symptoms: One-way audio is observed when a call goes through BACD and comes over SIP trunk.
Conditions: This symptom occurs when a call comes through SIP trunk and is connected to an agent phone via BACD during the third call transfer, along with the “headset auto-answer” configuration in the ephone.
Workaround: Remove the “headset auto-answer” configuration in the ephone configuration.

• CSCue06309
Symptoms: A Cisco 2900 series router running IOS 152-4.M1 may generate the following error message:
SYS-2-BADPOOL Attempt to use buffer with corrupt pool pointer, ptr= xxxxxxxx, pool= D0D0D0D0 -Process= "IGMP Snooping Receiving Process", ipl= x, pid= xxx
This results in a low memory condition in the IO pool and memory fragmentation.
Conditions: This symptom occurs when IGMP is enabled on the router and receives multicast traffic.
Workaround: There is no workaround. The router needs to be proactively reloaded to reclaim the memory.
- **CSCue36197**
  Symptoms: The Cisco 7600 router may crash while performing the NSF IETF helper function for a neighbor over a sham-link undergoing NSF restart.
  Conditions: This symptom occurs when a router is configured as an MPLS VPN PE router with OSPF as PE-CE protocol. OSPF in VRF is configured with a sham-link and a neighbor router over a sham-link is capable of performing an NSF IETF restart on sham-links.
  Note: This problem cannot be seen if both routers on sham-link ends are Cisco IOS routers.
  Workaround: Disable the IETF Helper Mode protocol by entering the following commands:

  ```
  enable configure terminal router ospf process-id [vrf vpn-name] nsf ietf helper disable end
  ```
  Note: Disabling Helper Mode will result in an OSPF peer dropping adjacency if the peer is reloaded.

- **CSCue55739**
  Symptoms: PfR MC/BR session may be flapped, if PfR learn is configured with scale configuration.
  Conditions: This symptom may be observed, if PfR traffic-classes are learned by PfR global learn configuration.
  Workaround: Disable PfR global learn by configuring `traffic-class filter access-list` pointing to the `deny ip ip any` ACL, and configure PfR learn “list”.

- **CSCue65130**
  Symptoms: The cmCallerID in CISCO-MODEM-MGMT-MIB is not updated when there is no CallerID.
  Conditions: This symptom is observed where incoming calls with no CID (Caller-ID) do not update the cmCallerID entry in the CISCO-MODEM-MGMT-MIB. When a call with no CID arrives, the CID from the previous caller stays in the MIB, which leads to an authentication bypass and produces billing errors.
  Workaround: There is no workaround.

- **CSCue94880**
  Symptoms: RTP traffic fails in reverse direction when an outside source list is configured and RTP SA IP matches against this list.
  Conditions: The symptom is observed with a Cisco IOS version above 12.4(9) mainline.
  Workaround: Use Cisco IOS Release 12.4(9).

- **CSCuf09006**
  Symptoms: Upon doing a `clear ip bgp * soft out` or `graceful shutdown` on a PE, all VPN v4 or v6 routes on an RR from this PE are purged at the expiry of enhanced refresh stale-path timer.
  Conditions: The symptom is observed with the following conditions:

  1. PE must have BGP peering with at least one CE (VRF neighbor) and at least one RR (VPN neighbor).
  2. PE must have a rtfilter unicast BGP peering with the RR.
  3. IOS version must have “Enhanced Refresh” feature enabled.
  4. A `clear ip bgp * soft out` or `graceful shutdown` is executed on the PE.
  Workaround: Instead of doing `clear ip bgp * soft out`, do a route refresh individually towards all neighbors.
Symptom: A vulnerability in the Resource Reservation Protocol (RSVP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger an interface queue wedge on the affected device.

The vulnerability is due to improper parsing of UDP RSVP packets. An attacker could exploit this vulnerability by sending UDP port 1698 RSVP packets to the vulnerable device. An exploit could cause Cisco IOS Software and Cisco IOS XE Software to incorrectly process incoming packets, resulting in an interface queue wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-rsvp

- CSCuf28733

Symptom: The Cisco IOS Software implementation of the network address translation (NAT) feature contains three vulnerabilities when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are not available.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-nat

Conditions: See advisory for details

Workaround: There is no workaround.

Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- CSCug31561

A vulnerability in the DHCP implementation of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability occurs during the parsing of crafted DHCP packets. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that has the DHCP server or DHCP relay feature enabled. An exploit could allow the attacker to cause a reload of an affected device.

Cisco has released free software updates that address this vulnerability. There are no workarounds to this vulnerability.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp
Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- CSCug66784
  Symptoms: DSP Fails to Recover Using “Test DSP Device 0 All Reset”.
  Conditions: A crashed DSP (LSI PVDM3) fails to recover via the CLI command `test voice dsp device 0 all reset`.
  Workaround: A complete reload of the router is required to recover the DSP.

**Resolved Caveats—Cisco IOS Release 15.2(2)T3**

Cisco IOS Release 15.2(2)T3 is a rebuild release for Cisco IOS Release 15.2(2)T. The caveats in this section are resolved in Cisco IOS Release 15.2(2)T3 but may be open in previous Cisco IOS releases.

- CSCsq83006
  Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.
  Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which are connected via a partial mesh port-channel.
  Workaround: Use the port-channel interface settings below:

```plaintext
(config)# interface port-channel <port-channel interface number>
(config-if)# bandwidth <bandwidth value>
(config-if)# delay <delay value>
```

Further Problem Description: If a test is done with a physical interface, not a port-channel, this issue is not seen.

- CSCtj59117
  Symptoms: The following error message is seen and the router freezes and crashes:

```plaintext
%SYS-2-BADSHARE: Bad refcount in retparticle
```

A reload is required to recover.

Conditions: The symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Release 12.4(15)T14.

Workaround: Remove CEF.

- CSCtj95182
  Symptoms: Scanning for security vulnerabilities may cause High CPU condition on Cisco Catalyst 3750.

Conditions: Network scanner run against a 3750 running 12.2.55.SE.

Workaround: There is no workaround.

Additional Information: Vulnerable versions: 12.2(52)EX through 12.2(55)SE4 15.1(3)T through 15.1(4)XB8a 15.2(1)GC - 15.2(3)XA.
First fixed in: 12.2(55)SE5, 15.0(1)EX, 15.1(1)SG, 15.2(1)E, 15.2(4)M, 15.3(1)T.  
In the meantime, Cisco has published several security advisories for Smart Install vulnerabilities:  
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall  
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smartinstall

- **CSCto32044**  
  Symptoms: The interface hangs and fails to pass traffic. It will still show an “up/up” status but the input and output rates will go to 0. The following errors will be seen:  
  %SBETH-3-ERRINT: GigabitEthernet0/0, error interrupt, mac_status = 0x0000040000000000  
  %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to reset  
  The interface number will vary.  
  Conditions: The conditions are unknown.  
  Workaround: There is no workaround.

- **CSCtq14253**  
  Symptoms: Joins/registers not forwarded to the RP when first configured.  
  Conditions: The symptom is observed when the router is first configured.  
  Workaround: Reload all routers in the setup.

- **CSCq17444**  
  Symptoms: A Cisco AS5400 crashes when performing a trunk call.  
  Conditions: The following conditions are observed:  
  - Affected Cisco IOS Release: 15.1(3)T.  
  - Affected platforms: routers acting as voice gateway for H.323.  
  Workaround: There is no workaround.

- **CSCtq91063**  
  Symptoms: A Cisco router may unexpectedly reload due to bus error or generate a spurious access.  
  Conditions: The issue occurs when fragmentation of a tunneled packet fails due to the F/S particle pool running out of free particles. The F/S pool is used for fragmentation, so this exhaustion of this pool will occur when there is a large amount of traffic flowing for which fragmentation is required.  
  By default, path MTU discovery is enabled for tunnels which means that fragmentation is done at the tunnel interface, rather than the underlying interface and this issue is not hit. If the MTU is overridden then it may become exposed to this issue. Assuming the tunnel is over an ethernet interface with MTU of 1500, then this will happen by setting the tunnel MTU to greater than 1476 bytes.  
  Workarounds:  
  1. Remove MTU override from the tunnel interface; or  
  2. Configure “service disable-ip-fast-frag”; or  
  3. Reduce hold queue sizes such that the total size of the queues for all active interfaces in the system does not exceed 512.

- **CSCtq70641**  
  Symptoms: When a router that is running a version before REL8, is rebooted with an IOS version having EIGRP REL8 onwards it does not show routes received from peer in EIGRP topology.
Conditions: Initially all the devices are running EIGRP version before REL8 (show eigrp plug shows that). Now when a device is booted with newer EIGRP version (REL8 onwards) and it comes up before its hold down timer is expired on peers then this issue is hit.

Workaround: There is no workaround.

- CSCts38674
  Symptoms: UUT/modem fails to make a call using external dialer interface.
  Conditions: The symptom is observed when the cellular interface is configured with “no ip address” and when using an external dialer interface, UUT/modem will fail to make a call.
  Workaround: Configure cellular interface with “ip address negotiated”.

- CSCts83046
  Symptoms: Back-to-back ping fails for P2P GRE tunnel address.
  Conditions: The symptom is observed when HWIDB is removed from the list (through list remove) before it gets dequeued.
  Workaround: There is no workaround.

- CSCtt17039
  Symptoms: UUT is reloaded with OSPFv3 IPsec authentication configured. The UUT has formed neighborship with two routers over port-channel.
  Conditions: The symptom is observed when the UUT is reloaded with OSPFv3 IPsec authentication configured.
  Workaround: There is no workaround.

- CSCtt97905
  Symptoms: Multiple demandNbrCallDetails traps generated.
  Conditions: Multiple demandNbrCallDetails traps are generated for connect under normal conditions.
  Workaround: There is no workaround.

- CSCtu08373
  Symptoms: Router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.
  Conditions: IOS firewall is configured and traffic is flowing through the router.
  Workaround: There is no workaround.

- CSCtu11013
  Symptoms: The router crashes when the SAF forwarder is enabled.
  Conditions: This symptom is observed when the SAF forwarder is enabled.
  Workaround: Disable the SAF forwarder.

- CSCtu21967
  Symptoms: A router configured to be an IP voice gateway may crash.
  Conditions: The exact conditions for this crash are currently unknown.
  Workaround: There is no workaround.

- CSCtu24740
Symptoms: A Cisco ISR router may unexpectedly reload due to bus error or Segv Exception or experience a spurious access.

Conditions: The symptom is observed when NAT and dampening are configured on the same interface while the device is running Cisco IOS Release 15.2(1)T or a later release.

Workaround 1: Remove dampening from the configuration.

Workaround 2: Downgrade to Cisco IOS Release 15.1(4)M or earlier release.

- CSCtu28696
  Symptoms: A Cisco ASR 1000 crashes with **clear ip route** *.
  Conditions: The symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, then clear the configuration.
  Workaround: There is no workaround.

- CSCtw48553
  Symptoms: When MPLS-IP is configured on a Cisco router and QoS policy-map actions are applied, classification fails and packets are dropped. This prevents the committed information rate (CIR) from getting updated on the output interfaces.
  Conditions: This symptom is observed on any Cisco router that is running Cisco IOS Release 15.0(1)M7.10 or later releases, or Cisco IOS Release 15.1(4) M2.5 or later releases.
  Workaround: There is no workaround.

- CSCtw86793
  Symptoms: A Cisco router running Cisco IOS 15.2T will generate phase II rekeys using IKEv1 instead IKEv2.
  Conditions: The symptom is observed with an IKEv2 DVTI hub (tunnel mode GRE IP).
  Workaround: Anchor the IKEv2 profile into the IPsec profile.

- CSCtx45373
  Symptoms: Under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command, the “VRF specified does not match this router” error message is displayed. When you issue the **redistribute eigrp 1** command, it gets NVGENd without AS number.
  Conditions: This symptom occurs under **router eigrp virtual-name** and **address-family ipv6 autonomous-system 1**, when you enter **af-interface Ethernet0/0** to issue a command and exit, and later, under **router bgp 1** and **address-family ipv4 vrf red**, you issue the **redistribute ospf 1** command.
  Workaround: Instead of using the **exit-af-interface** command to exit, if you give a parent mode command to exit, the issue is not seen.

- CSCty54695
  Symptoms: RRI routes are missing when IPsec SA is up after peer IP change.
  Conditions: This symptom is observed under the following conditions:
  - Cisco ASR 1002 router running Cisco IOS XE Release 3.4.2S.
  - Dynamic crypto map with RRI.
  - Peer changes the IP address frequently.
  Workaround: Clear the crypto session with the peer.
• CSCty61216
  Symptoms: CCSIP_SPI_Control causes leak with a Cisco AS5350.
  Conditions: The symptom is observed with the following IOS image:
c5350-jk9su2_ivs-mz.151-4.M2.bin.
  It is seen with an outgoing SIP call from gateway (ISDN PRI --> AS5350 --> SIP --> Provider SIP
gateway).
  Workaround: There is no workaround.

• CSCty82414
  Symptoms: A crash is seen.
  Conditions: The symptom is observed when all of ZBFW, SGFW, IPS and Scansafe are configured
  on the router and traffic as in the traffic profile is sent (http- [tcp], dhcp -[udp] traffic).
  Workaround: Unconfigure IPS.

• CSCty86039
  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with
  traffic going through some of the tunnels.
  Conditions: This symptom is seen with tunnel interface with QoS policy installed.
  Workaround: There is no workaround.

• CSCtz13465
  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.
  Conditions: This symptom is observed with an interface with a policy installed.
  Workaround: There is no workaround.

• CSCtz35999
  The Cisco IOS Software Protocol Translation (PT) feature contains a vulnerability that could allow
  an unauthenticated, remote attacker to cause a denial of service (DoS) condition.
  Cisco has released free software updates that address this vulnerability.
  Workarounds that mitigate this vulnerability are available.
  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-pt
  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes
  seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each
  Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the
  vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases
  that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.
  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security
  Advisory Bundled Publication” at the following link:

• CSCtz42421
  Symptoms: The device experiences an unexpected crash.
  Conditions: This symptom is observed when Zone-Based Firewalls are enabled. H225 and H323
  inspection is being done during the crash. The actual conditions revolving around the crash is still
  being investigated.
Caveats

Workaround: There is no workaround.

- **CSCtz47595**
  Symptoms: Dial string sends digits at incorrect times.
  Conditions: The symptoms are seen with a Cisco 3925 router running Cisco IOS Release 15.2(3)T using PVDM2-36DM modems with firmware version 3.12.3 connecting over an ISDN PRI to an analog modem.
  When using a dial string to dial an extension (or other additional digits), the modem should answer before the dial string is sent. If a comma is used, there should be a pause after connecting before sending the digits. The default value of the digital modem is one second per comma; two commas would be two seconds, three commas = three seconds and so on.
  1. With any number of commas in the string, debugs show the digits are sent at random intervals, sometimes before the call was answered and as much as up to 30 seconds after the call connects, i.e.: 919195551212x,22 or 1212x,,22.
  2. With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, i.e.: 919195551212x22.
  Dialing directly to a number with no extension or extra digits works as expected.
  Workaround: There is no workaround.

- **CSCtz58719**
  Symptoms: Watchdog timeout is seen under interrupt or process.
  Conditions: This symptom is observed with a QoS configuration applied. The issue happens because of resource contention between a process path packet and an interrupt path packet.
  Workaround: Disable QoS.

- **CSCtz58941**
  Symptoms: The router crashes when users execute the `show ip route XXXX` command.
  Conditions: This symptom is observed during the display of the `show ip route XXXX`, when the next-hops of “XXXX” networks are removed.
  Workaround: The `show ip route XXXX` command (without “XXXX”) does not have the problem.

- **CSCtz59145**
  Symptoms: A crash occurs randomly. The following error messages are often seen before the crash:
  Mar 31 16:30:16.955 GMT: %SYS-2-MALLOCFAIL: Memory allocation of 20 bytes failed from 0x644DA7E0, alignment 0 Pool: Processor Free: 274176384 Cause: Interrupt level allocation Alternate Pool: None Free: 0 Cause: Interrupt level allocation -Process=",<interrupt level>"", ipl= 1
  Mar 31 16:30:16.963 GMT: %SYS-3-BADLIST_DESTROY: Removed a non-empty list(707C0248, name: FW DP SIP dialog list), having 0 elements
  This device is not actually running out of memory. There is a memory action going on at the interrupt level which is not allowed.
  Conditions: This symptom occurs when Zone-Based Firewalls inspect SIP traffic. This issue is likely related to the tracebacks and error messages given above. The actual condition is still being investigated.
  Workaround: If plausible, disabling SIP inspection could possibly prevent further crashes.

- **CSCtz69084**
  Symptoms: The switch crashes when trying to enable IPsec MD5 authentication on the SVI.
  Conditions: This symptom is observed with the following conditions:
Caveats for Cisco IOS Release 15.2(2)T

1. Configure the IPsec MD5 authentication in global configuration mode.
   ipv6 router ospf 1
   area 0 authentication ipsec spi 1000 md5 123456ABCDEF123456ABCDEF123456AB

2. Configure the IPsec MD5 authentication as below in the interface mode with MD5 key 7 and device crashes.

   Workaround: There is no workaround.

- CSCtz71084

  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

  CE0---------PE0-------------------RR | | | | CE1---------PE1---------------|

  Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

  This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y.

  Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

  Workaround: Hard clear.

- CSCua21166

  Symptoms: Unable to form IPSec tunnels due to error: "RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license."

  Conditions: Even though the router does not have 225 IPsec SA pairs, error will prevent IPsec from forming. Existing IPsec SAs will not be affected.

  Workaround: Reboot to clear out the leaked counter, or install hsec9 which will disable CERM (Crypto Export Restrictions Manager).

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.8/2.3:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:M/C:N/I:N/A:P/E:U/RL:W/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:


- CSCua22789

  Symptoms: Router crashes while doing on-demand image download to switch which does not support Smart Install feature.

  Conditions: Router crashes while using CLI to upgrade the images on switch which does not support Smart Install feature.

  Workaround: There is no workaround.
CSCua39390
Symptoms: The PRI configuration (voice port) is removed after a reload:

```
interface Serial1/0:23
% Invalid input detected at '^' marker.
no ip address
% Incomplete command.
encapsulation hdlc
% Invalid input detected at '^' marker.
isdn incoming-voice voice
% Invalid input detected at '^' marker.
no cdp enable
% Invalid input detected at '^' marker.
voice-port 1/0:23
% Invalid input detected at '^' marker.
```

Also getting trace back:

```
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60702F38z 0x6070A300z
0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x607EE41Cz 0x607EE41Cz 0x607EE41Cz 0x607EE41Cz
Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T and Release 15.1(4)M4.
The issue is not occurring with Cisco IOS Release 12.4(24)T6 or lower. The issue occurs after reload.
Workaround: Reapply configuration after router comes back up.
```

CSCua40273
Symptoms: The ASR1k crashes when displaying MPLS VPN MIB information.

Conditions: Occurs on the ASR1K with version 15.1(02)S software.

Workaround: Avoid changing the VRF while querying for MIB information.

CSCua55629
Symptoms: SIP memory leak seen in the event SIPSPI_EV_CC_MEDIA_EVENT.

Conditions: The command `show memory debug leaks` shows a CCSIP_SPI_CONTORL leak with size of 6128 and points to the event “SIPSPI_EV_CC_MEDIA_EVENT”:

```
Adding blocks for GD...

I/O memory

Address  Size  Alloc_pc  PID  Alloc-Proc     Name
Processor memory

Address  Size  Alloc_pc  PID  Alloc-Proc     Name
286E144  6128  809528  398  CCSIP_SPI_CONTR CCSIP_SPI_CONTROL
```

Workaround: There is no workaround.

CSCua61330
Symptoms: Traffic loss is observed during switchover if,
1. BGP graceful restart is enabled.
2. The next-hop is learned by BGP.
Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.
Workaround: There is no workaround.

- CSCua67998
  Symptoms: System crashes.
  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.
  Workaround: There is no workaround.

- CSCua70065
  Symptoms: CUBE reloads on testing DO-E0 secure video call over CUBE when SDP passthru is enabled.
  Conditions: The symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.
  Workaround: There is no workaround.

- CSCua99969
  Symptoms: IPv6 PIM null-register is not sent in the VRF context.
  Conditions: This symptom occurs in the VRF context.
  Workaround: There is no workaround.

- CSCub05907
  Symptoms: Reverse routes are not installed for an IPsec session while using dynamic crypto map.
  Conditions: This symptom occurs when the remote peer uses two or more IP addresses to connect and it goes down and comes back at least twice.
  Workaround: Issue “clear crypto session” for that peer.

- CSCub10951
  Symptoms: At RR, for an inter-cluster BE case, there are missing updates.
  Conditions: This symptom is observed with the following conditions:
  1. The following configuration exists at all RRs that are fully meshed:
     - bgp additional-paths select best-external
     - nei x advertise best-external
  2. For example, RR5 is the UUT. At UUT, there is,
     - Overall best path via RR1.
     - Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called “ic_path_rr5”.
     - Initially, RR5 advertises “ic_path_rr5” to its nonclient iBGP peers, that is, RR1 and RR3.
  3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
  4. At PE6, reconfigure the route so that RR5 will have “ic_path_rr5” as its “best-external (internal) path”. At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.
Caveats

Workaround: Hard/soft clear.

- **CSCub18682**
  Symptoms: The phone number is missing in the Sent INVITE from CUBE when testing OutBound Dial-Peer Matching using the phone number and context under destination-uri.
  Conditions: This symptom occurs when running Cisco IOS Release 15.2(2)T1.12.
  Workaround: There is no workaround.

- **CSCub28913**
  Symptoms: The Cisco ISR G2 with VPN-ISM drops packets over an IPsec tunnel-protected tunnel interface.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T images, when there is a crypto map (static or dynamic) applied to the interface.
  Workaround:
  - Disable the ISM-VPN (issue “no crypto engine slot xx”, where xx is the slot number where the ISM is located).
  - Alternatively, change the configuration to use either static or dynamic VTIs for the tunnels where you need a crypto-map.

- **CSCub45809**
  Symptoms: Cisco IOS configured for Voice over IP may experience stack corruption due to multiple media loops.
  Conditions: This requires a special configuration of IP features along with disabling the recommended media flow-around command. IOS version 15.2(2)T
  Workaround: Apply media flow-around command.
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:U/RL:W/RC:C CVE ID CVE-2012-5044 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCub54872**
  Symptoms: A /32 prefix applied to an interface (e.g.: a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.
  Conditions: The symptom is observed when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).
  Workaround: Use a shorter prefix.
  Further Problem Description: This issue does not affect software switching platforms.

- **CSCub69976**
  Symptoms: Cisco 1941 in a DMVPN setup crashes with Cisco IOS Release 15.2(2)T2. The Cisco 2911 router and the Cisco 3945 router crash in a FlexVPN setup running Cisco IOS Release 15.3(00.14)T
  Conditions: This symptom occurs in a DMVPN setup and in the FlexVPN setup.
  Workaround: Disable the ISM module and switch to the onboard crypto engine using “no crypto engine slot 0”.

- **CSCub77062**
  Symptoms: The Cisco 2911 router and the Cisco 3945 router crash in a FlexVPN setup running Cisco IOS Release 15.3(00.14)T
  Conditions: This symptom occurs in a DMVPN setup and in the FlexVPN setup.
  Workaround: Disable the ISM module and switch to the onboard crypto engine using “no crypto engine slot 0”.

- **CSCub84770**
  Symptoms: The phone number is missing in the Sent INVITE from CUBE when testing OutBound Dial-Peer Matching using the phone number and context under destination-uri.
  Conditions: This symptom occurs when running Cisco IOS Release 15.2(2)T1.12.
  Workaround: There is no workaround.

Further Problem Description: This issue does not affect software switching platforms.
- **CSCub70336**
  Symptoms: The router can crash when “clear ip bgp *” is done in a large-scale scenario.
  Conditions: This symptom is observed only in a large-scale scenario, with tens of thousands of peers and several VPNv4/v6 prefixes.
  Workaround: “clear ip bgp *” is not a very common operation. Hence, this issue has not been observed by customers. The crash can only happen when “clear ip bgp *” is done. The workaround is not to execute “clear ip bgp *”.

- **CSCub84239**
  Symptoms: ISM-VPN (reventon) crash is observed.
  Conditions: The symptom is observed while reassembling ESP packets before decryption.
  Workaround: Disable ISM-VPN (reventon) and use either onboard crypto engine or software crypto engine.

- **CSCub84471**
  Symptoms: WAAS-optimized traffic is stuck in a loop when ISM VPN is enabled.
  Conditions: This symptom occurs when the ISM-VPN Module is turned on.
  Workaround: There is no workaround.

- **CSCub86706**
  Symptoms: After multiple RP switchover, the router crashes with the “UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO” error.
  Conditions: This symptom is observed with MVPN with 500 VRFs, when performing multiple switchovers on PE1.
  Workaround: There is no workaround.

- **CSCuc07799**
  Symptoms: The router crashes while booting with Cisco IOS Release 15.2(4)M weekly images.
  Conditions: This symptom occurs when the ISM-VPN Module is inserted in the router. WCCP and RG-Infra features are also enabled.
  Workaround: There is no workaround.

- **CSCuc42518**
  Symptoms: Cisco IOS Unified Border Element (CUBE) contains a vulnerability that could allow a remote attacker to cause a limited Denial of Service (DoS). Cisco IOS CUBE may be vulnerable to a limited Denial of Service (DoS) from the interface input queue wedge condition, while trying to process certain RTCP packets during media negotiation using SIP.
  Conditions: Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when certain sequence of RTCP packets is processed. All the calls on the affected interface would be dropped.
  Workaround: Increase the interface input queue size. Disable Video if not necessary.
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/3.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:OF/RC:C CVE ID CVE-2012-5427 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
- **CSCuc56259**
  Symptoms: A Cisco 3945 that is running 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen:

  ```
  %VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times and
  Delivery Ack could not be sent due to lack of buffers.
  ```

  Conditions: This happens when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

  Workaround: Check the configurations for any misconfigurations, especially with calls involving CUBE and CUCM.

- **CSCuc67033**
  Symptoms: A Cisco IOS router with the ISM VPN encryption module enabled can experience memory corruption-related crashes.

  Just before the crash, the router may display some syslog error messages related to the ISM VPN module:

  ```
  Aug 21 15:55:22: !!! Cannot find Revt counters struct for flowid: 0x4400012A
  Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A
  Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A
  ```

  Here, the word “Revt” is specific for the ISM VPN module.

  Also, some generic syslog error messages related to memory allocation failures may be displayed the crash:

  ```
  Aug 21 15:55:33: %SYS-3-BADBLOCK: Bad block pointer DD7D7D0 - Traceback= 23B9EA7Cz
  23BA1A44z 23BA1E24z 23B7128Bz 23B7129Cz Aug 21 15:55:33: %SYS-6-MTRACE: mallocfree: addr, pc 352791C4, 22DB4A50 352791C4, 3000006C 38808760, 2627EDF0 34C91824, 262724A8
  352791C4, 22DB6214 352791C4, 22DB4A50 352791C4, 3000006C 352791C4, 22DB6214 Aug 21 15:55:33: %SYS-6-MTRACE: mallocfree: addr, pc 352791C4, 22DB4A50 352791C4, 3000006C 352791C4, 22DB6214 3875D9C4, 600002CA 3875D5E0, 2627EDF0 35092ACC, 262724A8
  352791C4, 22DB4A50 352791C4, 3000006C Aug 21 15:55:33: %SYS-6-BLKINFO: Corrupted next pointer blk DD7D7D0, words 32808, alloc 214E636C, InUse, dealloc 0, rfcnt 1
  ```

  Conditions: This symptom is observed with the following conditions:

  - The ISM VPN crypto acceleration module is installed, enabled, and used for crypto operations (IPsec, etc.).
  - Cisco IOS supports ISM VPN (Cisco IOS Release 15.2(1)T1 or later releases).

  Workaround: Disable the ISM VPN module. The crash is specific to ISM VPN.

- **CSCuc82992**
  Symptoms: The router crashes upon execution of “no crypto engine slot 0”. when RG-infra feature is enabled.

  Conditions: This symptom occurs when RG-Infra and ISM-VPN are configured and when issuing “no crypto engine slot 0”.

  Workaround: There is no workaround.

- **CSCud02361**
  Symptoms: Sequence number of spoofed ACK sent to the server has a 0x00 value.

  Conditions: Once the max-incomplete high is reached, when the next SYN packet is sent from the client, the UUT sends a SPOOFED-ACK after getting the SYN-ACK from the server. When this ACK packet is observed at the server agent with the packets tool, the sequence number is found to be 0x00.
Resolved Caveats—Cisco IOS Release 15.2(2)T2

Cisco IOS Release 15.2(2)T2 is a rebuild release for Cisco IOS Release 15.2(2)T. The caveats in this section are resolved in Cisco IOS Release 15.2(2)T2 but may be open in previous Cisco IOS releases.

- **CSCsg48725**
  
  **Symptoms:** A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:
  
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)

  **Conditions:** This symptom is observed on a Cisco platform when TACACS accounting and authorization is enabled and when the TACACS server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

- **CSCsy93069**
  
  **Symptoms:** After a period of telepresence calls, tracebacks and then a router crash is seen.

  **Conditions:** The symptom is observed only when running Cisco IOS firewall with l7 SIP inspect policies applied. This crash happens at low scale with one CTS 3k call cycling with a hold time of 600 secs. It occurs intermittently and over time in an environment where there may be some call failures.

  Workaround: There is no workaround.

- **CSCtj10515**
  
  **Symptoms:** Crash seen in IGMP input process.

  **Conditions:** The symptom is observed in a multi-VRF scenario with extranet MVPN.

  Workaround: There is no workaround.

- **CSCtj48387**
  
  **Symptoms:** After a few days of operation, an ASR router running as an LNS box crashes with DHCP related errors.

  **Conditions:** DHCP must be enabled and sessions should be getting DHCP information from a RADIUS server.

  Workaround: There is no workaround.

- **CSCtq24557**
  
  **Symptoms:** Router crash after deleting multiple VRFs. This happens very rarely.

  **Conditions:** The symptom is observed in a large scale scenario.

  Workaround: There is no workaround.

- **CSCtq99664**
  
  **Symptoms:** Traffic does not egress from the interface.

  **Conditions:** The VRF set on the interface is originally configured for IPv4 and IPv6 address family. If the VRF is reconfigured to remove the IPv4 address family, then all interfaces in that VRF stop sending traffic.

  Workaround: Shut down and re-enable the interface in question.
- **CSCtr22434**
  Symptoms: Stale IPsec policy is not cleared and the same SPI cannot be used until you reload. Memory leak of crypto acl is also observed.
  Conditions: The symptom is observed with “OSPFv3 ipsec authentication” configured on in the interface.
  Workaround: Use a different SPI or reload the router.

- **CSCtr45287**
  Symptoms: Router crashes in a scale DVTI scenario.
  Conditions: The symptom is observed when the IPsec tunnel count reaches around 2500.
  Workaround: Use fewer tunnels or use a different platform.

- **CSCtr86328**
  Symptoms: A device running Cisco IOS might reload when the web browser refreshes/reloads the SSL VPN portal page.
  Conditions: Cisco IOS device configured for clientless SSL VPN.
  Workaround: There is no workaround.

  Further Problem Description: This problem has been seen when the stock Android browser visits the SSL VPN portal (after authentication) and refreshes (reloads) the page. However, the issue is not browser-specific and other browsers might trigger the issue too.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/6.5:
  
  
  CVE ID CVE-2012-1344 has been assigned to document this issue.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

- **CSCtr87070**
  Symptoms: Enable login failed with error “% Error in authentication”.
  Conditions: The symptom is observed with TACACS single-connection.
  Workaround: Remove TACACS single-connection.

- **CSCts00341**
  Symptoms: When executing a CLI that requires domain-name lookup such as `ntp server server.domain.com`, the command fails with the following message on the console:

  ASR1k(config)#ntp server server.domain.com <<< DNS is not resolved
  with dual RPs on ASR1k
  Translating 'server.domain.com'...domain server (10.1.1.1) [OK]

  %ERROR: Standby doesn't support this command

  ASR1k(config)#do sh run | i ntp
  ASR1k(config)#

  Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

  Workaround: Instead of using `hostname` in the command, specify the IP address of the host.
CSCts32708
Symptoms: Similar to CSCth80642, IOS SSLVPN router fails to accept new sessions. The users will not be able to load the webvpn login page. If you enable debug sdps you may see: Sev 4:sdps_get_pak_from_tcp(), line 1080:tcp_getpacket returned error 2, tcb=0x6A9EFFEC
Conditions: The router remains reachable otherwise (ie you can ping the webvpn IP) SSL process is running and listening on the right port. “Show tcp tcb” and “show tcp brief all numeric” will show connections stuck in CLOSED and CLOSEWAIT state. Clearing the tcp tcb sessions does not restore connectivity Taking webvpn in/out of service does not restore connectivity Disabling webvpn cef and rebooting does not prevent the issue Rebooting does resolve the issue temporarily
Workaround: 1. Reboot. 2. If available for your platform, get the fix for CSCth80642 AND disable webvpn cef (you should reboot or clear the tcb connections after disabling webvpn cef). This may prevent the problem.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1:
https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-3286 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

CSCts34693
Symptoms: A Cisco router may crash with the following error message:
000199: %BGP-5-ADJCHANGE: neighbor x.x.x.x Up
Exception to IOS Thread:
Frame pointer 0x30CF1428, PC = 0x148FDF84
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog
-Traceback=
1#07279b80de945124c720ef5414c32a90 :10000000+48FDF84 :10000000+48FE400 :10000000+4B819C8 :10000000+4B81964 :10000000+P5FAD8 :10000000+P5FD10 :10000000+P5FE P0 :10000000+P5FF94 :10000000+F60608
Conditions: This symptom is observed with a Cisco ASR 1004 router running Cisco IOS Release 15.0(1)S. This problem appears to be related to an EEM script that executes on a syslog event.
event manager applet BGP-MON
  event tag BGP-DOWN syslog pattern "BGP-5-ADJCHANGE.*Down"
event tag BGP-UP syslog pattern "BGP-5-ADJCHANGE.*Up"
trigger
corrrelate event BGP-DOWN or event BGP-UP
action 02 cli command "enable"
action 03 cli command "sh log"
action 04 mail server "$_email_server" to "$_email_to" from "$_info_routername@mcen.usmc.mil" subject "Problems on $_info_routername, BGP neighbor Change" body "$_cli_result"
Workaround: There is no workaround.

CSCts72911
Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the non-restarting peer (RR, in this case).
Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.
Workaround: There is no workaround.
• CSCtt17762
  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.
  Conditions: The symptom is observed on an IP PIM multicast network.
  Workaround: There is no workaround.

• CSCtt23358
  Symptoms: RP reset @ __be_tunnel_protection_remove_idb_for_connection in flexVPN scale setup.
  Conditions: The symptom is observed with a shut/no shut on a flex tunnel and then executing the command clear crypto session.
  Workaround: There is no workaround.

• CSCtt26208
  Symptoms: A Cisco 3845 running Cisco IOS Release 15.1(4)M1 may have a processor pool memory leak in CCSIP_SPI_CONTROL.
  Conditions: Not known at this time.
  Workaround: There is no workaround.

• CSCtt26692
  Symptoms: A Cisco router reloads with the warm-reboot command.
  Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.
  Workaround: There is no workaround. Remove “warm-reboot” from configuration (router will not be able to use warm reboot feature).

• CSCtt43552
  Symptoms: A Cisco router reloads with the warm-reboot command.
  Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.
  Workaround: There is no workaround. Remove “warm-reboot” from configuration (router will not be able to use warm reboot feature).

• CSCtt43843
  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.
  Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.
  Workaround: There is no workaround.
• CSCtt46730
  Symptoms: Platform crashes during IKEv2 negotiation between the spoke and the hub with Cisco TrustSec (CTS) enabled on the Cisco 3945E platform.
  Conditions: This symptom is seen with re-negotiation of IKEv2 SA between the peers.
  Workaround: There is no workaround.

• CSCtt47007
  Symptoms: Router is unstable and displays badshare error messages in the syslog:
  Conditions: Has been seen on a Cisco ISR 3845 with AIM-SSLV3. It may also show on other platforms as well.
  Workaround: Disable WebVPN CEF and reload the router.

• CSCtt95505
  Symptoms: The router crashes after configuring OSPF routing protocol.
  Conditions: The crash occurs after:
  1. Configuring OSPF with a summary prefix.
  2. Deconfiguring OSPF; and then
  3. Configuring OSPF again. For example:

  ```
  ipv6 router ospf 1
  router-id 1.1.1.1
  summary-prefix 2001:0db8:1:1::/64
  redistribute connected

  no ipv6 router ospf 1

  ipv6 router ospf 1
  router-id 1.1.1.1
  summary-prefix 2001:0db8:1:1::/64
  redistribute connected
  ```
  Workaround: There is no workaround.

• CSCtt96597
  Symptoms: Unable to power-cycle modem using `test cellular unit modem-power-cycle`.
  Conditions: The symptom is observed when a router cannot communicate with the modem due to a possible modem firmware crash or device disconnect.
  Workaround: Reload router.

• CSCtu07626
  Symptoms: Router processing SIP traffic crashes.
  Conditions: The following error may be seen prior to the crash:

  `%SDP-3-SDP_PTR_ERROR: Received invalid SDP pointer from application. Unable to process.`
  Workaround: There is no workaround.

• CSCtu19450
  Symptoms: A system that is running Cisco IOS may reload when a large number of routes are simultaneously deleted at the same time that the inetCidrRouteTable is being walked.
Caveats

Conditions: This symptom is only likely to happen when there are large numbers of interfaces and routes within the system, and when large numbers of routes are being rapidly removed, and the system is loaded, at the same time that the inetCidrRouteTable is being walked.

Routes may be deleted from the system both directly, and also indirectly for example, when a significant number of PPPoE sessions are removed.

Workaround: Avoid walking the inetCidrRouteTable while significant numbers of routes are being removed from the routing system.

- CSCtu25150
  
  Symptoms: A Cisco router acting as a voice gateway may unexpectedly reload due to a SegV exception or bus error, or may experience a spurious access.
  
  Conditions: The exact conditions leading to the crash are not known. The issue is only present in Cisco IOS Release 15.1(4)M and later.
  
  Workaround: There is no workaround.

- CSCtu29881
  
  Symptoms: A router may crash while using double authentication for IPsec (ESP + AH) and certain types of traffic.
  
  The following message is seen in the crashinfo file:

  validblock_diagnose, code = 1
  current memory block, bp = 0xZZZZZZZZ, memorypool type is I/O data check, ptr = 0xZZZZZZZZ
  next memory block, bp = 0xZZZZZZZZ, memorypool type is I/O data check, ptr = 0xZZZZZZZZ
  previous memory block, bp = 0xZZZZZZZZ, memorypool type is I/O data check, ptr = 0xZZZZZZZZ
  
  The router crashes due to I/O memory corruption - block overrun.
  
  Conditions: The symptom is observed with double authentication (AH + ESP) and certain type of packets.
  
  Workaround 1: Do not using double authentication (AH + ESP). Use ESP instead.
  
  Workaround 2: Use an IOS version that does not have the fix for CSCtc40806.

- CSCtu32301
  
  Symptoms: Memory leak may be seen.
  
  Conditions: This is seen when running large show commands like show tech-support on the linecard via the RP console.
  
  Workaround: Do not run the show commands frequently.

- CSCtu38244
  
  Symptoms: After bootup, the GM cannot register and is stuck in “registering” state. Issuing the clear crypto gdoi command is required for a successful registration to the keyserver.
  
  Conditions: The symptom is observed upon router bootup.
  
  Workaround: Either do a clear crypto gdoi after a reload, or configure a second keyserver entry. This does not have to be an existing keyserver, it can be just a dummy address.

- CSCtu43120
  
  Symptoms: Service accounting start is not sent for L2TP sessions.
  
  Conditions: This symptom is observed with L2TP.
  
  Workaround: There is no workaround.
- **CSCtv21900**
  Symptoms: Intermittent one-way audio occurs from an MGCP gateway to a Cisco IP phone.
  Conditions: This symptom is observed under the following conditions:
  - Encrypted call with SRTP.
  - MGCP Controlled Gateway.
  - Cisco IOS Release 15.1(4)M or later releases.
  Phone logs show the following message:
  code 7
  3
  The “Rcvr Lost Packet” counter on the Cisco IP phone begins to increment as soon as the call connects.
  Workaround 1: Downgrade the software to Cisco IOS Release 15.1(3)T or earlier releases.
  Workaround 2: Perform a hold/resume on the one-way audio call. This mitigates the problem.

- **CSCtw41214**
  Symptoms: ACEs are not source IP translated in multidomain authentication (MDA) mode.
  Conditions: The symptom is observed in MDA mode.
  Workaround: There is no workaround.

- **CSCtw46229**
  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.
  Conditions: The symptom is observed with PPP negotiations and the session involving PPPoA.
  Workaround: Ensure all your PPP connections stay stable.

- **CSCtw55976**
  Cisco IOS Software contains a vulnerability in the Intrusion Prevention System (IPS) feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist.
  Cisco has released free software updates that address this vulnerability.
  Workarounds that mitigate this vulnerability are available.
  This advisory is available at the following link:

- **CSCtw56439**
  Symptoms: The `ip mtu` command that is configured on an IPsec tunnel disappears after a router reload.
  Conditions: The symptom is observed with IPsec and the `ip mtu` over a tunnel interface.
  Workaround: There is no workaround.

- **CSCtw58664**
  Symptoms: SSL VPN for SCCP causes a crash when clearing a WebVPN session.
  Conditions: The symptom is observed when using the SSL VPN for SCCP phones feature and when clearing the WebVPN session:
clear webvpn session context SSLVPNphone

[WV-TUNL-EVT]:[0] Returning address 10.0.112.200 to pool
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x2601227C
-Traceback= 0x26008B3Cz 0x25F9D7E8z 0x25F94A3Cz 0x224B66A8z 0x224BCBA8z
0x224CBF70z 0x23D22684z 0x23D189C0z 0x237F0144z 0x237F0128z -Traceback=
0x26008B3Cz 0x25FCEAA8z 0x238561D8z
The frequency of the issue is rare.

Workaround: There is no workaround.

- CSCtw59086
  Symptoms: Unable to connect via Cisco AnyConnect or the WebVPN portal on a Cisco IOS router.
  The following message is seen in the Syslog: %SSLVPN-6-LICENSE_NO_FREE_COUNT: All available SSLVPN session licenses are in use
  Conditions: This symptom is observed when the WebVPN License counter incorrectly reads 4294967295. Also, no connections are visible while executing the show webvpn session context all command.
  For example:
  
  sh webvpn session context all
  show webvpn license
  Max platform license count : 1500
  Available license count : 100
  Reserved license count : 100
  * In-use count : 4294967295
  Workaround: Reload the Cisco router.

- CSCtw62310
  Symptoms: The cells keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service-policy”.
  Conditions: The symptom is observed when removing the policy-map from map-class.
  Workaround: There is no workaround.
  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw71564
  Symptoms: Not all data packets are accounted for in the “show stats” output of the video operation.
  Conditions: The symptom is observed with heavy load on the responder caused either by many video sessions or other processes.
  Workaround: Reduce processor load on device running the responder.

- CSCtw73544
  Symptoms: A leak is observed in the header pool with “ppp multilink”.
  Conditions: This symptom is observed with PPP over ATM
  Workaround: There is no workaround.

- CSCtw78064
  Symptoms: The display-logout message on a Cisco SCCP Phone is not cleared even after pressing other buttons on the phone.
Caveats for Cisco IOS Release 15.2(2)T

Conditions: This symptom is observed on the Cisco SCCP phone (also known as Skinny Phone or ePhone) when the last extension mobility (EM) user in a hunt group logs out using the HLog button. This symptom is observed even if the last EM user logs out of the hunt group and logs back in.

Workaround: There is no workaround.

- CSCtw84664
  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.
  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.
  This advisory is available at the following link: [Cisco Security Advisory](http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip)

- CSCtw87132
  Symptoms: A Cisco router may crash when clearing a TCP session:
  ```
  router120#clear tcp tcb 08C5F4F8
  [confirm]
  SIGBUS (0xFFF1BD460) : Bus Error ( [0xD0D0D39] invalid address alignment)
  ```
  Conditions: This has been experienced on a Cisco 2921 router that is running Cisco IOS Release 15.1(4)M through to Release 15.1(4)M3.
  Workaround: There is no workaround.

- CSCtw95189
  Symptoms: The “%Unknown DHCP problem. No allocation possible” error is observed in the DHCP error log.
  Conditions: This symptom occurs when open access is enabled and the supplicant is authz failed. Then, DHCP IP address assignment does not take place.
  Workaround: There is no workaround.

- CSCtx01604
  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.
  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.
  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx04709
  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.
  Conditions: This symptom is seen when a multiple route goes down at the same time, and query arrives from neighbor router. Finally, neighbor detects SIA for affected router and neighbor state is flap. However, active entry is remaining after that, and route is not updated.
  Workaround: The `clear ip eigrp topology network mask` command may remove unexpected active entry.
Caveats

- **CSCtx19332**
  Symptoms: A Cisco router crashes when “remote mep” is unlearned while auto EOAM operations are executing.
  Conditions: This symptom is observed if “remote mep” is unlearned from the auto database (shutdown on interface or remote mep reload) while the “IP SLA ethernet-monitor jitter” operation is still running. The crash occurs if the initial control message times out.
  Workaround: There is no workaround.

- **CSCtx22322**
  Symptoms: If an over-temperature interrupt occurs when the CPU utilization is high, the system may crash.
  Conditions: The symptom is observed when CPU utilization of the system is high Cisco 880 series routers.
  Workaround: There is no workaround.

- **CSCtx29543**
  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the `show ip route` command.
  Conditions: This symptom occurs under the following conditions:
  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.
  The router may now crash when doing `show ip route` command or when default route is updated.
  Workaround: There are two possible workarounds:
  1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

- **CSCtx32329**
  Symptoms: When using the `show ipv6 rpf` command, the router crashes or displays garbage for RPF idb/nbr.
  Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.
  Workaround: Do not use static multicast routes, or make sure that the next hop specified can always be resolved. Do not use the `show` command.

- **CSCtx32527**
  Symptoms: The `show crypto session` command reveals the flexVPN GRE tunnel is in a DOWN state instead of DOWN-negotiating.
  Conditions: The symptom is observed with “ip address negotiated” configured on the GRE tunnel interface (with tunnel protection). The tunnel is unable to reach the gateway initially.
  Workaround: Configure an IP address on the tunnel interface instead of “ip address negotiated”.

- **CSCtx32628**
  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.
Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

- BGP full mesh is configured.
- BGP cluster-id is configured.
- `address family vpnv4` is enabled.
- `address family ipv4 mdt` is enabled.
- The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

Workaround: Remove the cluster-id configuration or hard-reset the bgp session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- **CSCtx45970**

  Symptoms: A crash is seen only in the negative case, when the frequency is not a multiple of history interval.

  Conditions: The symptom is observed when the value is not initialized.

  Workaround: Configure the right configuration with frequency being the multiple of interval.

- **CSCtx47213**

  Symptoms: The following symptoms are observed:
  1. Session flap when iBGP local-as is being used on RRs.
  2. Replace-as knob is not working in iBGP local-as case.

  Conditions:
  1. The session will flap when iBGP local-as is used on the RR client and RR sends an update.
  2. Replace-as knob even used is ignored and prefixes are appended with local-as.

  Workaround: Do not use iBGP local-as.

- **CSCtx51935**

  Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

  Conditions: The symptom is observed with the following steps:

  ```
  interface gi1/2
  mpls traffic-eng tunnels
  no shut

  router OSPF 1
  mpls traffic-eng area 100
  mpls traffic-eng router-id lo0
  end
  ```

  ```
  show mpls traffic-eng link-management summary
  ```

  Workaround: There is no workaround.

- **CSCtx54882**

  Symptoms: A Cisco router may crash due to Bus error crash at voip_rtp_is_media_service_pak.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2.

  Workaround: There is no known workaround.

- **CSCtx57784**
Symptoms: Device crashes while configuring “logging persistent url”.
Conditions: Occurs when the destination file system has zero free bytes left.
Workaround: There is no workaround.

- CSCtx64347
  Symptoms: Despite open access being configured on the port, traffic to/from the client is blocked.
  Conditions: This symptom occurs when an authenticating port with open-access and multi-auth hostmode configured, is interrupted.
  Workaround: There is no workaround.

- CSCtx64684
  Symptoms: While configuring the ISIS on two Cisco 2921 routers connected back to back, the ISIS neighbors do not come up.
  Conditions: This symptom is observed only on the SVI interface. This issue is only seen with EHWIC.
  Workaround: If the router has an L3 port, form a neighborship on a physical interface directly or create dot1q subinterfaces if peering is required on multiple VLANs.

- CSCtx65979
  Symptoms: A Cisco 2801 cannot boot up using -adv enterprisek9-mz images or higher starting with Cisco IOS interim Release 15.2(2.15)T. Reports insufficient memory to load the image.
  Conditions: The symptom is observed at boot up.

- CSCtx66030
  Symptoms: A Cisco router handling SIP registrations/unregistrations may unexpectedly reload. This symptom is observed on the following devices:
  - SIP-CME
  - SIP-SRST GW
  - CUBE
  Conditions: This symptom is observed when the number of SIP registrations/unregistrations handled is more than 320.
  Workaround: Limit the number of registrations/unregistrations to less than 320.

- CSCtx66046
  Symptoms: The Standby RP crashes with a traceback listing db_free_check.
  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.
  Workaround: Before removing the address, remove the network statement which covers the address of the loopback interface.

- CSCtx66804
  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFFREQ.
  Conditions: The symptom is observed with the following conditions:
– “PPP LCP Delay 0” is configured.
– The symptom can be seen on Cisco IOS Release 15.0(1)M2.

Workaround: Set delay timer without 0.

- **CSCtx67474**
  Symptoms: Update message is sent with an empty NLRI when the message consists of 2-byte aspath in AS-PATH attribute and 4-byte value aggregate attribute.
  Conditions: This can happen when there is a mix of 2-byte and 4-byte attributes in the update message and the message is sent from a 2-byte peer and there is a 4-byte aggregator attribute.
  Workaround: Move all the 2-byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- **CSCtx74342**
  Symptoms: After interface goes down or is OIReD, in a routing table you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next hop interface set to the interface that is down.
  Conditions: The symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).
  Workaround: Configuring SPF throttle timer can change the interval.
  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Router show ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS Interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDP - ND Prefix, DCE - Destination, NDR - Redirect
       L - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/64 [110/10]
    via Ethernet0/0, directly connected
```

- **CSCtx86539**
  Symptoms: NAT breaks SIP communication with addition of media attributes.
  Conditions: The symptom is observed with NAT of SIP packets.
  Workaround: There is no workaround.

- **CSCtx87646**
  Symptoms: Firmware behavior options can only be used if “service internal” is activated.
  Conditions: The condition under which this symptom is observed is unknown.
  Workaround: There is no workaround.

- **CSCtx90705**
  Symptoms: Several MPLS features fail for ping.
  Conditions: The symptom is observed during ISSU downgrade.
  Workaround: There is no workaround.

- **CSCtx92802**
  Symptoms: IP fragmented traffic destined for crypto tunnel is dropped.
  Conditions: The symptom is observed under the following conditions:
- Cisco IOS Release 15.0(1)M7 on a Cisco 1841.
- VRF enabled.
- CEF enabled.
- VPN tunnel.
Workaround: Disable VFR or CEF.

- CSCty01234
  Symptoms: A router running Cisco IOS may reload unexpectedly.
  Conditions: This symptom is observed only with low-end platforms using VDSL interfaces, such as a Cisco 887 router. It also requires that the **qos pre-classify** command be used in conjunction with IPSec and GRE, such as in a DMVPN configuration.
  Workaround: Do not use the **qos pre-classify** command.

- CSCty02403
  Symptoms: An EIGRP topology entry with bogus next-hop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus next-hop. So if you have a default route received from some neighbors, then that default route will also flap.
  Conditions: It can only occur when more then one attribute set in any route received from a neighbor.
  Workaround: Do not set more then one attribute in the route.

- CSCty03745
  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.
  Conditions: This symptom occurs when the IPv4 default route exists, that is:
  ```
  ip route 0.0.0.0 0.0.0.0 <next-hop>.
  Or a certain static/IGP route exists: For example:
  ip route 0.0.253.0 255.255.255.0 <next-hop>.
  ```
  Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family.
  For example:
  ```
  router bgp 65000
  address-family l2vpn vpls
    neighbor 10.10.10.10 next-hop-self
  ```
  Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty05092
  Symptoms: EIGRP advertises the connected route of an interface which is shut down.
  Conditions: This symptom is observed under the following conditions:
  1. Configure EIGRP on an interface.
  2. Configure an IP address with a supernet mask on the above interface.
  3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.
  Workaround 1: Remove and add INTERFACE VLAN xx.
  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty05150
Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.

Conditions: This symptom occurs when the stub ABR is configured in a VRF without “capability vrf-lite” configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.

Workaround: Remove and reconfigure “area x stub”.

- CSCty12083
  Symptoms: A Cisco 819 router with the C819HG+7 SKU reloads.
  Conditions: This symptom is observed on a Cisco 819 router with the C819HG+7 SKU reloads while running Cisco IOS Release 15.1(4)M3.8.
  Workaround: There is no workaround.

- CSCty21638
  Symptoms: The Cisco 3945 router crashes with the base configuration of SAF/EIGRP.
  Conditions: This symptom occurs when enabling the SAF Forwarder on the Cisco 3945 router.
  Workaround: There is no workaround.

- CSCty30185
  Symptoms: Call transfer to an element crashes if one of the element’s number is invalid.
  Conditions: The issue is observed when call is transferred to parallel hunt group.
  Workaround: There is no workaround.

- CSCty32851
  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to “multilink ppp”.
  Conditions: The symptom is observed when the interface is configured with a VRF.
  Workaround: Shut down the interface before making the encap configuration change.

- CSCty37445
  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.
  Conditions: The symptom is observed when on the spoke you have a distribute list route-map command setting tags.
  Workaround: Once you remove that command EIGRP works normally.

- CSCty42626
  Symptoms: Certificate enrollment fails for some of the Cisco routers due to digital signature failure.
  Conditions: This symptom was initially observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.
  This issue potentially impacts those platforms with HW crypto engine. Affected platforms include (this is not a complete/exhaustive list)
  - c3925E, c3945E
  - c2951, c3925, c3945
  - c7200/VAM2+/VSA, possibly VPNSPA on c7600/cat6K
  - 819H ISR G2 routers with ISM IPSec VPN accelerator
Workaround: There is no workaround.

- **CSCty43587**
  Symptoms: Crash observed with memory corruption similar to the following:
  
  ```bash
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX, dealloc XXXXXXXX
  ```
  Conditions: The symptom is observed when SIP is configured on the router or SIP traffic is flowing through it.
  Workaround: There is no workaround.

- **CSCty48870**
  Symptoms: Router crash due to a bus error.
  Conditions: This has been observed in router that is running Cisco IOS Release 15.2(2)T and 15.2(3)T with NBAR enabled on a crypto-enabled interface. NBAR can be enabled through NAT, QoS, or NBAR protocol discovery.
  Workaround: Using `no ip nat service nbar` will help where NBAR is enabled through NAT.

- **CSCty53243**
  Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.
  Conditions: This symptom is observed when CUBE changes the video port to “0” in 200 OK sent to the UAC.
  Workaround: There is no workaround.

- **CSCty54434**
  Symptoms: ISRG2 with ISM VPN is not bringing up more than one tunnel in a crypto map-based scenario with large certificates (4096 bit).
  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T and Cisco IOS Release 15.2(2)T.
  Workaround: Configure IKEv2 fragmentation so that the fragmentation/reassembly is handled by IKE code rather than by IPsec.

- **CSCty56850**
  Symptoms: Routers are not updating the cnpdAllStatsTable with traffic from all expected protocols.
  Conditions: The symptom is observed with routers that are running Cisco IOS 15.x (tested in 15.0, 15.1 and 15.2(2)T).
  Workaround 1: Use the following CLI to get the stats for all the protocols:
  ```
  show IP NBAR protocol-discovery
  ```
  Workaround 2: Perform a snmpget against objects in cnpdAllStatsTable.

- **CSCty58992**
  Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.
  Conditions: This symptom is observed under the following conditions:
  - Cluster is in v6 mode.
– A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3 (SIP POTS), which is when the issue occurs.

Workaround: There is no workaround.

• CSCty64721

Symptoms: Improper memory allocation by CTI process crashes the CME.

Conditions: The CTI front end process is using up huge memory causing the CME to crash eventually. When the crash occurs:

Processor Pool Total: 140331892 Used: 140150164 Free: 181728
I/O Pool Total: 27262976 Used: 5508816 Free: 21754160

Workaround: There is no workaround.

• CSCty65189

Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

Conditions: The symptom is observed when ZBFW is configured.

Workaround: There is no workaround.

• CSCty65334

Symptoms: Unconfigured crypto ACL causes the Cisco 3900 router to crash.

Conditions: This symptom is observed with a Cisco 3900 image with ISM crypto engine installed and enabled. This may also affect the Cisco 2900 and Cisco 1900 routers with ISM crypto engine installed and enabled.

Workaround: When changing the crypto ACL configuration, disable the ISM crypto engine first using the `no crypto engine slot 0` command, and then change the ACL. After changing the ACL, reload the router with ISM enabled.

• CSCty68348

Symptoms: If the OSPF v2 process is configured with the `nsr` command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

Conditions: This symptom is observed under the following conditions:

– The OSPF router is configured for “nsr”.
– Shutdown/no shutdown of the OSPF process.

Workaround: Flapping of the neighbor will fix the issue.

• CSCty77190

Symptoms: DTLS is switched back to TLS after reconnect.

Conditions: This symptom is observed with the following conditions:

– Test image c3845-advsecurityk9-mz.152-2.T1.InternalUseOnly
– Test version - Cisco IOS Release 15.2(01)T

Workaround: Restart the AnyConnect client.

• CSCty78435

Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.
Caveats

Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty805o53
  Symptoms: Multicast router crashes.
  Conditions: The symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.
  Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- CSCty94289
  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.
  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.
  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty96052
  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.
  Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.
  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty97784
  Symptoms: The router crashes.
  Conditions: This symptom is observed when NBAR is enabled, that is, “match protocol” actions in the QoS configuration, or “ip nbar protocol-discovery” on an interface or NAT is enabled and “ip nat service nbar” has not been disabled.
  Workaround: There is no workaround.

- CSCty98834
  Symptoms: The Cisco c2900, c3900, and c1900 IOS with the ISM VPN crypto engine might crash after some time when you run out of memory on the ISM VPN engine as there are memory leaks during rekey.
  Conditions: This symptom occurs when the ISM VPN crypto engine is enabled.
  Workaround: Disable the ISM VPN module using the no crypto engine slot 0 command.

- CSCtz13818
  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.
  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.
  Workaround 1: Refresh the updated route-target to use clear ip route vrf vrf-name net mask.
Workaround 2: Hard clear the BGP session with the peer.

- **CSCtz25364**
  
  Symptoms: GM to GM communication between ISM VPN and the Cisco ASR 1000 series router with TBAR enabled is broken.

  Conditions: This symptom occurs when ISM VPN and the Cisco ASR 1000 series router are GMs and TBAR is enabled.

  Workaround: Disable ISM VPN or disable TBAR and switch to counter-based anti-replay.

- **CSCtz25953**
  
  Symptoms: “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

  Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- **CSCtz27137**
  
  Symptoms: An upgrade to the S639 or later signature package may cause a Cisco IOS router to crash.

  Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:
  - Cisco IOS Release 12.4(24)T4
  - Cisco IOS Release 15.0(1)M4
  - Cisco IOS Release 15.0(1)M8
  - Cisco IOS Release 15.2(3)T

  Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:
  - Access the router via the console.
  - Enter break sequence to access ROMmon mode.
  - Change the config-register value to 0x2412.
  - Boot the router to bypass the startup-configuration.
  - Configure the basic IP parameters.
  - TFTP a modified configuration to the router's running-configuration with Cisco IOS IPS disabled.
  - Reset the config-register to 0x2102.
  - Enter the **write memory** command and reload.

- **CSCtz44989**
  
  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

  Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.

  Workaround: There is no workaround.

- **CSCtz51773**
Symptoms: High CPU seen on routers equipped with an ISM-VPN module. The output of `show process cpu` shows that the process “REVT Background” is using around 70% of the CPU cycles. The ISM-VPN module is not visible in `show diag`, and the output of `show crypto engine configuration` indicates that the module status is DEAD.

Conditions: The symptom is observed with an ISM VPN with a few IPSec tunnels. This can take between a day and a week.

Workaround 1: Reload the router.

Workaround 2: For a longer-run workaround and if the traffic volume is not too high, switch to the onboard crypto hardware using the configuration `no crypto engine slot 0`.

- **CSCtz70623**
  
  Symptoms: A Cisco router may experience a software-forced crash.

  Conditions: Crash may occur when a 2-wire cable is unplugged from the G.SHDSL interface.

  Workaround: There is no workaround.

- **CSCtz70938**
  
  Symptoms: When the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.

  Conditions: This symptom occurs when the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.

  Workaround: Do not use boot configuration files other than startup-configuration when there are “service-module” CLI in the configuration.

- **CSCtz72044**
  
  Symptoms: EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.

  Conditions: The issue is timing-dependent, therefore the problem is not systematic.

  Workaround: There is no workaround.

- **CSCtz80643**
  
  Symptoms: A PPPoE client’s host address is installed in the LNS’s VRF routing table with the `ip vrf receive vrf name` command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the `ip vrf receive vrf name` command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- **CSCtz99916**
  
  Symptoms: The Cisco 3945 router does not respond to a reinvite from CVP.

  Conditions: This symptom occurs when call legs are not handled in a proper IWF container.

  Workaround: There is no workaround.

- **CSCua06598**
  
  Symptoms: Router may crash with breakpoint exception.

  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.
Workaround: Disable SNMP IPv6 polling.

- CSCua07791
  Symptoms: A Cisco ISR G2 running Cisco IOS Release 15.2(2)T or later shows a memory leak in the CCSIP_SPI_CONTRO process.
  Conditions: The leak is apparent after 3-4 weeks. The process is CCSIP_SPI_CONTRO.
  Workaround: There is no workaround.

- CSCua31157
  Symptoms: One way traffic is seen on a DMVPN spoke-to-spoke tunnel one minute after the tunnel is built. Issue is only seen intermittently.
  Logs on the spoke that fails to receive the traffic show “Invalid SPI” error messages exactly one minute after the tunnel between the spokes came up.
  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T1.
  Workaround: There is no workaround.

- CSCua39107
  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.
  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.
  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- CSCua43930
  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.
  Conditions: The issue is seen on a Cisco ISR G2.
  Workaround: There is no workaround.

- CSCua44462
  Symptoms: DNS reply is not cached.
  Conditions: DNS based X25 routing. DNS server is reachable via IPsec over Gig link and SHDSL links. There are Cisco devices at different locations. Few of them are communicating to DNS server via IPsec over Gig link and few of them are communicating via IPsec over ATM (EHWIC-4SHDSL-EA and HWIC-4SHDSL). It is seen that the UDP reply contains the x25 address to IP address resolution but it is not being used by the router causing X25 calls to fail.
  Workaround: There is no workaround.

- CSCua47570
  Symptoms: The show ospfv3 event command can crash the router.
  Conditions: The symptom is observed when “ipv4 address family” is configured and redistribution into OSPFv3 from other routing protocols is configured.
  Workaround: Do not use the show ospfv3 event command.
Resolved Caveats—Cisco IOS Release 15.2(2)T1

Cisco IOS Release 15.2(2)T1 is a rebuild release for Cisco IOS Release 15.2(2)T. The caveats in this section are resolved in Cisco IOS Release 15.2(2)T1 but may be open in previous Cisco IOS releases.

- CSCtn07696
  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the `show tech-support` command output using the `ftp` command due to TCP-2-INVALDTCB.
  Conditions: This symptom is observed with the following command:
  ```bash
  show tech-support | redirect ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt
  ```
  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.
  Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCto59459
  Symptoms: Connections that are optimized by WAAS are reset. Malformed TCP options are added to the packet that is created and sent by WAAS-Express over the WAN, causing the peer WAE to reset connections.
  Conditions: Any TCP connection will suffer from this defect.
  Workaround: There is no workaround.

- CSCto71671
  Symptoms: Using the `radius-server source-ports extended` command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.
  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.
  Workaround: There is no workaround.

- CSCto93880
  Symptoms: Enable authentication fails when user is configured with TACACS server group.
  Conditions: This symptom occurs when TACACS server is configured with user defined group and configured for enable authentication. User is unable to authenticate when he tries to switch to privilege executive mode (enable) and gets an error that indicates that there is no address for defined servers.
  ```bash
  %TAC+: no address for get_server %TAC+: no address for get_server
  ```
  Workaround: Configure the TACACS server group with the default group name.

- CSCtq12007
  Symptoms: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.
  Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less sever; you may see one every other packet drop, until the next rekey or tunnel reset.
  Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.
  Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the `clear crypto session` command or resetting all the tunnels.
Caveats for Cisco IOS Release 15.2(2)T

• CSCtq59923
  Symptoms: OSPF routes in RIB point to an interface that is down/down.
  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.
  Workaround: Configure the `ip routing protocol purge interface` command.

• CSCtq64987
  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
  An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.
  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

• CSCtr46123
  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.
  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.
  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

• CSCtr47642
  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the `bgp additional-paths select best-external` command, a specific prefix may not have bestpath calculated for a long time.
  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:
  1. Configure: `bgp additional-paths install` under vpnv4 AF
  2. Configure: `bgp additional-paths select best-external`
  Immediately disable backup path calculation/installation using the `no bgp additional-paths install` command.
  The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.
  Workaround: Configure the `bgp additional-paths install` command and the `bgp additional-paths select best-external` command with a delay of 10 seconds.
Caveats for Cisco IOS Release 15.2(2)T

- CSCtr86149
  Symptoms: A router crashes if placing a call from an ISDN phone to an IP phone. The call is a secure SIP call (TLS); the phone is also using secure SCCP.
  Conditions: The router is in secure SRST mode due to a WAN outage.
  Workaround: There is no workaround.

- CSCtr88739
  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.
  Symptom 2: The routes in BGP may not get installed to RIB.
  Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.
  For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.
  For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.
  Workaround for symptom 1: Remove “import-route target” and reconfigure route-target.
  Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCtr94471
  Symptoms: Carrier specific exec commands under cellular interface, such as profile configuration and activation commands, return an error.
  Conditions: The symptom is observed after the router boots up.
  Workaround: There is no workaround.

- CSCts11344
  Symptoms: Upon a reload, a router will crash during bootup.
  Conditions: The symptom is observed on a Cisco 3900 series router with “no cry eng slot 0” configured then the configuration is saved in the startup config file. The issue is seen upon a reload.
  Workaround: Do not save “no cry eng slot 0” in the config file. If you want to turn off the crypto engine, do it after router boot up.
  Further Problem Information: To recover from the crash, first reload an image build before 07/07/2011. Remove “no cry eng slot 0” from the startup configuration then reload the image you are going to use. After the router boots up, configure “cry eng slot 0” to turn off the engine.

- CSCts27042
  Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.
  Conditions: The symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).
  Workaround: There is no workaround.

- CSCts31111
  Symptoms: Coredump generation fails on the Cisco 800.
Conditions: This symptom occurs when coredump is configured.

Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:

```
cf t
config-reg 0x0
end
wr
reload
yes
<rommon prompt>
DISABLE_WATCHDOG=yes
sync
set
conf-reg 0x2102
reset
```

- **CSCts38429**

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:


- **CSCts44718**

  Symptoms: A router may crash.

  Conditions: The crash may occur when a service policy that has a flow monitor as an action is applied to a virtual interface and that virtual interface is deleted. It may also occur when the service policy is applied to a physical interface that is removed by OIR.

  Workaround: Before deleting (or OIRing) the interface, remove the flow monitor from the policy or the policy from the interface.

- **CSCts46578**

  Symptoms: Firewall may drop a packet with log similar to:

  `%FW-6-DROP_PKT: Dropping ftp-data session 10.7.7.99:1449 10.7.8.100:20 due to Invalid Seq# with ip ident 6621 tcpflags 0x8018 seq.no 3558493868 ack 1386495675

  Retransmitted packet is allowed through.`

  Conditions: CBAC configured.

  Workaround: There is no workaround.

- **CSCts56044**

  Symptoms: A Cisco router crashes while executing a complex command. For example:

  `show flow monitor access_v4_in cache aggregate ipv4 precedence sort highest ipv4 precedence top 1000`

  Conditions: This symptom is observed while executing the `show flow monitor top` top-talkers command.

  Workaround: Do not execute complex flow monitor top-talker commands.

- **CSCts63501**

  Symptoms: The non-EOS forwarding path for the explicit null label (reserved label 0) is programmed as drop on the linecard, resulting in PW traffic loss with an MPLS LDP explicit-null configuration.
Caveats for Cisco IOS Release 15.2(2)T

Conditions: The PW traffic loss occurs on linecards in which MPLS LDP explicit-null is set.
Workaround: There is no workaround.

- CSCts63973
  Symptoms: Router configured with ScanSafe can crash with high session testing. This happens very rarely and is not seen frequently.
  Conditions: The symptom is observed when ScanSafe is configured and HTTP sessions are created at a high rate.
  Workaround: There is no workaround.

- CSCts67465
  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.
  Conditions: The symptom is observed always, if the standby is configured as an SSO.
  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts70790
  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.
  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.
  Workaround: Remove and re-add the `neighbor default-originate` command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCts76410
  Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.
  Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Release 15.0(1)M7.
  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts78348
  Symptoms: Packet drop will occur on a router when the interface is configured as 10/full.
  Conditions: It seems that when interface is configured as 10/full, with the traffic of 10 Mbps, this issue will occur. By performing a shut/no shut on the interface, this issue will recover but it will be seen again when you reload the device.
  This issue may be seen on a Cisco 19xx and a Cisco 29xx (except Cisco 2951). This issue may occur when manual set duplex on the affected platform.
  Workaround 1: Perform a shut/no shut on the interface and this issue will recover.
  Workaround 2: Use auto negotiation.

- CSCts85459
  Symptoms: Upon a reload, the cellular interface will not negotiate if a crypto map is applied to it.
Caveats for Cisco IOS Release 15.2(2)T

Conditions: The symptom is observed on a Cisco 881 router that has a cellular interface which dials to get an IP address and also acts as the VPN gateway. When we reload the router, the cellular interface does not connect if a crypto map is applied and we see IPsec fails to initialize because we do not have an IP address.

Workaround: This situation remains until we manually remove the crypto map from the cellular interface. Then we see the chat-script starting and the whole dialing procedure starts, then the cellular link is up with an IP address. Then we re-apply the crypto map again and the tunnel works fine.

- CSCts97925
Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.
Conditions: This symptom is observed only with IPv6, and not with IPv4.
Workaround: Disable IPv6 CEF.

- CSCts99818
Symptoms: Traceback is seen.
Conditions: The symptom is observed when multimode ADSL/VDSL CPE configuration is rapidly changed between VDSL and ADSL mode while using a VDSL2-only transmission mode profile on DSLAM.
Workaround: There is no workaround.

- CSCtt02313
Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.
Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.
Workaround: There is no workaround.

- CSCtt03207
Symptoms: Traffic flows through unauthorized supplicant switch
Conditions: Authenticator Switch should have established auto-config with authorized supplicant switch. Now bring up, unauthorized supplicant switch by physically connecting to hub placed between ASW & SSW. Though wrong dot1x credential is used, ASW allows network access for unauthorized SSW.
Workaround: None.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 2.9/2.4:


No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:


- CSCtt05316
Symptoms: Under show content-scan sessions active, the user group information is printed over and over.
Caveats

Conditions: The symptom is observed when the TCP SYN is retransmitted.

Workaround: There is no workaround.

- CSCtt05910
  Symptoms: Router crashes.
  Conditions: The symptom is observed when running the `show sum` command. It is seen with the Cisco 3900e platform.
  Workaround: Do not use the `show sum` command.

- CSCtt11210
  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.
  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.
  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.
  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- CSCtt13401
  Symptoms: The following traceback is seen:
  %SYS-2-NOBLOCK: suspend with blocking disabled. -Process= "ESWPPM", ipl= 0, pid= 67
  Conditions: This issue occurs when CISP/NEAT auto-config code starts.
  Workaround: There is no workaround.

- CSCtt16051
  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.
  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.
  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

- CSCtt17785
  Symptoms: In the output of `show ip eigrp nei det`, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.
  Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).
  Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- CSCtt17879
  Symptoms: The `bgp network backdoor` command does not have any effect.
Conditions: This symptom occurs:
- On 64-bit platform systems.
- When the network is learned after the backdoor has been configured.
Workarounds: Unconfigure and reconfigure the network backdoor.

- CSCtt19027
  Symptoms: When ACL is applied to the serial interface or Gigabit interface, ping failure seen even though the permit statement is there.
  Conditions: The symptom is observed when ACL is configured on the serial interface or Gigabit interface.
  Workarounds: Enable EPM by installing the security license.
  Further Problem Description: This is seen with those images where EPM is not supported and because of that an EPM call always gives a return value as “deny” due to registry call.

- CSCtt21681
  Symptoms: MAC learning stops once the supplicant is authorized to an auth-fail VLAN.
  Conditions: This symptom occurs in an MDA setup and when an auth-fail VLAN is configured on the port.
  Workarounds: There is no workaround.

- CSCtt23038
  Symptoms: IOSD crashes while executing the “show flow monitor name monitor2” command after an RP downgrade on bay 0.
  Conditions: This symptom is observed during a Cisco ASR 1004 ISSU downgrade from MCPDEV to Cisco IOS XE Release 3.5.
  Workarounds: There is no workaround.

- CSCtt26074
  Symptoms: Memory leak with IP SLAs XOS Even process.
  Conditions: The symptom is observed with IP SLA configured.
  Workarounds: There is no workaround.

- CSCtt28703
  Symptoms: VPN client with RSA-SIG can access a profile where his CA trustpoint is not anchored
  Conditions: Use of RSA-SIG.
  Workarounds: Restrict access by using a certificate-map matching the right issuer.
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.5/3:
  No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

- CSCtt28764
  Symptoms: Throughput and connection rate are degraded by 50 percent.
Conditions: This symptom is observed when static ip-sgt bindings are configured without ZBFW or IPsec configurations on Cisco ISR G2 routers.

Workaround: There is no workaround.

- CSCtt35936
  Symptoms: EIGRP route updates are not sent to DMVPN spokes. The `show ip eigrp inter` command output shows pending routes in interface Q, which remains constant. The `show ip eigrp int deta` command output shows that the next sequence number of the interface remains the same (does not advance).
  Conditions: This symptom occurs when EIGRP session flapped, resulting in routes being withdrawn and restored.
  Workaround: Add a static route on any spoke that kicks out EIGRP learned routes from the RIB table; this will again kick the interface on the HUB.

- CSCtt36513
  Symptoms: Crash seen on a Cisco ASR for the process IPSec key engine.
  Conditions: The symptom is observed when you have more than 4K sessions up on the ASR.
  Workaround: There is no workaround.

- CSCtt43896
  Symptoms: Traffic is not flowing in the failed/running state when the port is in Open Access mode.
  Conditions: This symptom is observed when authorization fails or when in the running state and the port is open.
  Workaround: There is no workaround.

- CSCtt45381
  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
  An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.
  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

- CSCtu57226
  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

- **CSCt98801**
  - Symptoms: Mobile router reports stale RRP received from HA.
  - Conditions: The symptom is observed when the mobile router sends a RRQ to HA in CCOA mode.
  - Workaround: There is no workaround.

- **CSCtu06894**
  - Symptoms: Cisco UBE crashes when the “show sip-ua calls” command is executed while there is an active SIP call through system.
  - Conditions: This symptom is present on Cisco 2821 routers. The router crashes only when Cisco UBE receives an SDP length greater than 9000 bytes as part of a SIP message. And at the same time, if the show command is executed, the crash occurs. Otherwise, the crash is not seen.
  - Workaround: There is no workaround.

- **CSCtu11677**
  - Symptoms: A Cisco router may unexpectedly reload due to bus error or segV exception or generate a spurious error when the cSipStatsSuccessOkTable snmp object is polled.
  - Conditions: This is seen on a voice gateway when the cSipStatsSuccessOkTable snmp object is polled.
  - Workaround: Create an SNMP view and then block the oid for cSipStatsSuccessOkTable and then apply it to all SNMP communities on the device:
    ```
    snmp-server view blockmib iso include
    snmp-server view blockmib 1.3.6.1.4.1.9.9.152.1.2.2.5 exclude
    ```
    and then apply it to the community:
    ```
    snmp-server community <community> view blockmib ro
    ```

- **CSCtu17006**
  - Symptoms: Mediatrace is not working because RSVP fails to select the output interface.
  - Conditions: This symptom is observed only with PFR configuration.
  - Workaround: Remove the PFR configuration.

- **CSCtu17228**
  - Symptoms: DHCPv6 relay does not work on an EHWIC.
  - Conditions: This symptom is observed when one of the following modules is used.
    - EHWIC-4ESG
    - EHWIC-4ESG-P
    - EHWIC-D-8ESG
    - EHWIC-D-8ESG-P
  - Workaround: There is no workaround.
• CSCtu18712
  Symptoms: The MAB URL redirection feature does not work on Cisco ISR G2 platforms.
  Conditions: This symptom is observed when the URL redirect ACL is downloaded from ACS based on client credentials.
  Workaround: There is no workaround.

• CSCtu18786
  Symptoms: Device may crash showing “VOIP” error messages. Decodes point to voice functions.
  Conditions: The symptom is observed when SIP is enabled on the device.
  Workaround: There is no workaround.

• CSCtu28990
  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.
  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.
  Workaround: There is no workaround.

• CSCtu29107
  Symptoms: While using the “Reuse MAC address” feature on an ATM RBE, the router uses the MAC address of the main interface rather than the configured MAC address of the subinterface.
  Conditions: This symptom is observed when ATM route bridge encapsulation is used with the “Reuse MAC address” feature.
  Workaround: There is no workaround.

• CSCtu36224
  Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.
  Conditions: This symptom is observed on a Cisco router that is used for SSLVPN.
  Workaround: There is no workaround.

• CSCtu36321
  Symptoms: A voice session terminates abruptly when a data device is connected or disconnected behind a phone and the IAB feature is active.
  Conditions: The IAB feature is configured with “authentication event server dead action authorize voice” and:
  - RADIUS connectivity is down.
  - The voice device authenticates after RADIUS connectivity goes down.
  - The voice call is in progress.
  - The data device is connected/disconnected behind the phone.
  The connection/disconnection of the data device may cause the voice session to terminate.
  Workaround: There is no workaround. However, the call may be re-established immediately by the user.

• CSCtu41137
  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.
  Conditions: The core is observed while doing unconfiguration.
  Workaround: There is no workaround.
• CSCtu43731
Symptoms: On an RP1, RP switchover causes an RP reset.
Conditions: This symptom is observed with RP switchover under the following conditions:
  – The router must be an RP1.
  – The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.
An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.
Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.
Workaround 2: Do not enable FNF monitoring.

• CSCtu52820
Symptoms: A memory leak is observed under HTTP PROXY Server process.
Conditions: Device is configured with Cisco ISR Web Security with Cisco ScanSafe and has User Authentication NTLM configured.
Workaround: None.
PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:
CVE ID CVE-2011-4661 has been assigned to document this issue.
Additional information on Cisco’s security vulnerability policy can be found at the following URL:

• CSCtv52031
Symptoms: Router crashes while accessing the usergroup database.
Conditions: The symptom is observed with performance testing.
Workaround: There is no workaround.

• CSCtw45055
Symptom: A Cisco ASR router may experience a crash in the BGP Scheduler due to a segmentation fault if BGP dynamic neighbors have been recently deleted due to link flap. For example:

Nov 10 08:09:00.238: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
Nov 10 08:10:20.944: %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time expired) x bytes
Nov 10 08:10:20.944: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down
Nov 10 08:10:20.945: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted
Nov 10 08:10:34.328: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted
Nov 10 08:10:51.816: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
Exception to IOS Thread: Frame pointer 0x3BE784F8, PC = 0x104109AC
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler

The scheduler process will attempt to reference a freed data structure, causing the system to crash.
Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.
Workaround: There is no workaround.

- CSCtw45592
Symptoms: The “ntp server <DNS-name>” command is not synced to the standby. When the “no ntp server <hostname>” command is issued later on the active, the standby reloads because the config was not added.
Conditions: When the device is reloaded or when the DNS name is not resolved, the config is not added. After the standby SYNC failure, then issuing the “no ntp server <hostname>”.
Workaround: Use the IP/IPv6 addresses instead of the hostname for NTP configurations.

- CSCtw50141
Symptoms: Incremental leaks at __be_ber_get_stringa pointing to LDAP process.
Conditions: The symptom is observed when NTLM authentication is being used with an LDAP server and with the router acting as the NTLM proxy.
Workaround: There is no workaround.

- CSCtw58586
Symptoms: IKEv2 CLI configuration currently requires to manually link the crypto IKEv2 profile default to the crypto IPSec profile default. This enhancement request will change the behavior and create an automatic anchorage.
Conditions: This symptom is seen in IKEv2 usage.
Workaround: There is no workaround.

- CSCtw60333
Symptoms: HTTP process hangs. This impacts the webauth authentication scaling factor.
Conditions: The symptom is observed when the `clear ldap server server-name` command issued or the connection is closed during any outstanding LDAP. Transactions are in progress or are waiting for an LDAP response from the LDAP server.
Note: It is not only related to the secure-server. It is also applicable with an IP HTTP server. So generally it is applicable if you are using webauth with LDAP as the authentication server.
Workaround: Do not issue `clear ldap server` when any LDAP transactions for web authentication are in progress.

- CSCtw66262
Symptoms: The “security-group” command is missing after the match filter while configuring a class map. The customer cannot use the CTS ZBFW feature.
Conditions: This symptom is observed on the Cisco 890 platform.
Workaround: There is no workaround.

- CSCtw67283
Symptoms: A router receives either an “Illegal access to a low address” or an “Unexpected exception to CPU” crash depending on the platform. The crash occurs within several minutes of starting traffic.
Conditions: The router is configured with NBAR2, FNF, and HQoS. While running a mix of HTTP, FTP, SMTP, and DNS traffic, the router crashes within several minutes of starting traffic. The crash has been seen on the Cisco 891, 1941, and 2901 (Cavium based), but has not been seen on the Cisco 2951, 3925, or 3945.
Workaround: There is no workaround.
• CSCtw71620
  Symptoms: ISM VPN module cannot handle SSL records of a size greater than 1500 bytes. It will lead to SSL record encrypt/decrypt operation failure and result in a packet drop.
  Conditions: The symptom is observed with ISM VPN and SSL records of a size greater than 1500 bytes.
  Workaround: Disable the ISM VPN module with no crypto engine slot 0.

• CSCtw76044
  Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.
  Conditions: The symptom is observed under all conditions.
  Workaround: There is no workaround.

• CSCtw88094
  Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.
  Conditions: This symptom occurs shortly after the “ip sla schedule X start specific_start_time” command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.
  Workaround: Unschedule the probe before rescheduling for a specific start time.

• CSCtw99290
  Symptoms: The source or destination group-address gets replaced by another valid group-address.
  Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.
  Workaround: There is no workaround.

• CSCtx01604
  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.
  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.
  Workaround: Do not use any dynamic network interface IP address as CNS ID.

• CSCtx06018
  Symptoms: Interface queue wedge is seen when performing WAAS performance test.
  Conditions: The symptom is observed when performing WAAS performance test.
  Workaround: Increase interface input queue hold size.

• CSCtx06801
  Symptoms: Certain websites may not load when content-scan is enabled. Delays of up to a few seconds may be seen.
  Conditions: The symptom is observed when content-scan is enabled.
  Workaround: Though not always, refreshing the page sometimes helps.
Further Problem Description: The problem is due to GET request being segmented. For example, a huge get request of 1550 may come from the client in two different packets such as 1460+90=1550.

- CSCtx12216
  Symptoms: I/O pool memory goes low.
  Conditions: The symptom is observed with Scansafe configured. A small buffer is not getting freed.
  Workaround: There is no workaround.

- CSCtx16040
  Symptoms: ISM VPN card will crash when used in combination with SSL-AO of WAAS express.
  In theory, this can also happen in normal VPN-SSL.
  Conditions: The symptom is observed with high numbers of SSL connections.
  Workaround: Disable the ISM VPN card.

- CSCtx29557
  Symptoms: A standby crashes @ fib_fib_src_interface_sb_init.
  Conditions: All.
  Workaround: There is no workaround.

- CSCtx37680
  Symptoms: All the ports on the Cisco ISR are used up. After this we may see a crash.
  Conditions: The symptom is observed with ports on the Cisco ISR.
  Workaround: Ensure that not all the TCP ports on the Cisco ISR are allocated.

- CSCtx38806
  Symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.
  This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)
  The problem affects Firefox also (version 10.0.1) displaying the following message:
  “The page isn’t redirecting properly”
  Conditions: This symptom is observed on Cisco IOS that is acting as head end for SSL VPN connections.
  Workaround: Any of the following workarounds will work:
  1) Use the clientless portal to start the client. This only works in some versions of Cisco IOS software.
  2) Uninstall the update.
  3) Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:
     webvpn gateway gateway-name ssl encryption rc4-md5
  4) Use AC 2.5.3046 or 3.0.3054.
  5) Use older versions of Firefox (9.0.1).

Further Problem Description: For AnyConnect users, the following user error message is seen:
“Connection attempt has failed due to server communication errors. Please retry the connection”

The AnyConnect event log will show the following error message snippet:

```plaintext
Function: ConnectIfc::connect Invoked Function: ConnectIfc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
```

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:


- **CSCtx44060**
  - Symptoms: Flexvpn spoke-to-spoke tunnels do not come up.
  - Conditions: None.
  - Workaround: Once tunnels fail to come up, clear the NHRP cache on one spoke alone.

- **CSCtx46741**
  - Symptoms: ISM VPN module crashes for SSL records between 1800 bytes to 1840 bytes.
  - Conditions: The symptom is observed with an ISM VPN module + SSLVPN or ISM VPN + WAAS SSL AO.
  - Workaround: Disable ISM VPN module and fallback to onboard/SW crypto engine.

- **CSCtx47493**
  - Symptoms: NTLM authentication does not work.
  - Conditions: The symptom is observed when “ip admission ntlm rule” is configured on the interface.
  - Workaround: There is no workaround.

- **CSCtx88093**
  - Symptoms: A dialer idle timeout is not initiated after the watched route is installed back in the routing table while using a dialer watch list, causing the watch disconnect timer to not start.
  - Conditions: This symptom occurs while using the “dialer-list x protocol ip deny” command to define interesting/uninteresting traffic and while there is traffic flowing over the dialer interface.
  - Workaround: Use the method that follows to define interesting traffic instead of “dialer-list x protocol ip deny”:
    access-list x protocol ip deny dialer-list 1 protocol ip list x

- **CSCtx90299**
  - Symptoms: The DMVPN IPsec sessions might get torn down and unable to re-establish themselves after experiencing link-flap events.
  - Conditions: In a scaled DMVPN environment, when physical-port link-state up/down events happen, there will be stormed IPSec events to tear down and/or re-negotiate the sessions; it might run into a bad state that it cannot establish new sessions. Hence, when those active sessions expire (by time period or volume based), it can no longer be re-created. After some period of time, no more active session remains on the router.
  - Workaround: Reload the router.
- CSCty03629
  Symptoms: Traffic from a client with a valid IP-SGT mapping is dropped by the firewall.
  Conditions: NAT is co-located with SGFW1.
  Workaround: There is no workaround.

- CSCty04384
  Symptoms: IMA-DSLAPP crashes when doing interoperability testing with third-party DSLAMs.
  Conditions: Change line rates on CO sides with various loop lengths.
  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(2)T

All the caveats listed in this section are open in Cisco IOS Release 15.2(2)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCej11786
  Symptoms: A Cisco 2600 router reloads when a clear counter is performed on the router. This crash is reproducible only after making a number of calls first.
  Conditions: This symptom has been observed on a Cisco 2600 router.
  Workaround: There is no workaround.

- CSCtd63264
  Symptoms: A router may refuse configuration of certain VRF-aware translations (ip nat outside source static network global-network local-network mask vrf name extendable match-in- vrf) complaining that the translation already overlaps with an existing one, even though the configuration is valid and should be accepted.
  Conditions: The symptom is observed with certain VRF-aware translations.
  Workaround: There is no workaround.

- CSCtj59117
  Symptoms: The following error message is seen and the router freezes and crashes:
  %SYS-2-BADSHARE: Bad refcount in retparticle
  A reload is required to recover.
  Conditions: The symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Release 12.4(15)T14.
  Workaround: Remove CEF.

- CSCtq29120
  Symptoms: Authenticated MAC address is found in the MAC table even after the port is shut down.
  Conditions: The symptom is observed after the port is shut down.
  Workaround: There is no workaround.

- CSCtq39602
  Symptoms: DMVPN tunnel is down with IPSec configured. The `show dmvpn` command from the spoke shows the state is IKE.
  Conditions: After heavy traffic was pumping from DMVPN hub to spoke for some time: from a few minutes to a couple of hours.
Workaround: Configuring “crypto ipsec security-association lifetime kilobytes disable” to disable volume-based rekeying will reduce the problem.

- **CSCtq97723**
  
  Symptoms: A Cisco 3945 router may have performance issues (lower throughput) due to overruns.
  
  Conditions: This is seen with a steady bi-directional 64byte ICMP stream:
  
  
  - At 283Mbps = 37.16% wire rate of 1 gig overruns began to increment.
  
  Workaround: There is no workaround.

- **CSCtr07508**
  
  Symptoms: Unexpected reload after enabling WAAS on the interface.
  
  Conditions: The conditions have not been determined; router had just been reloaded, no traffic was flowing or special configuration done. Was seen several times in regression during a period of time, then ceased to happen in newer versions. Issue may be related with previous configuration on the router. It was not consistent.
  
  Workaround: There is no workaround.

- **CSCtr44373**
  
  Symptoms: This is a platform independent issue. Users cannot receive a call through a BRI port. A fast tone will be heard.
  
  Conditions: This symptom is observed on a newly released image.
  
  Workaround: Configure “forward digital all” in the CLI.
  
  The following example shows a sample configuration:
  
  ```console
  dial-peer voice 111 pots
  destination-pattern 111
  !direct-inward-dial
  port 2/0
  forward-digits all
  ```

- **CSCtr63128**
  
  Symptoms: A Cisco 2951 crashes with “Unexpected exception to CPU: vector 1400, PC = 0x55629DC , LR = 0x5562948” and following traceback:
  
  ```text
  - Traceback:
    0x55629DC
    0x5977F740 0x5584BC40 0x55841340 0x55079880 0x5509DB80 0x83D0DE80 0x83D82C40 0x67F14A80 0x67F6EB80 0x67F71500 0x87ADE040 0x87AD7DC0
    0x87AFB000 0x87B08300 0x87B09100
  ```
  
  Conditions: The symptom is observed with a Cisco 2951 router that is configured with IPSec/GRE tunnels with QoS and netflow configured. Not seen on the Cisco 3925 and Cisco 1921 which were tested with identical conditions.
  
  Crash seen when maximum multicast throughput is reached with the following traffic mix: packet size of 66, 256, 512, and 1024 bytes with a weight of 40, 30, 5, and 21 respectively.
  
  Issue not seen with the following traffic mix: packet size 66, 570, 594, and 1420 bytes with a weight of 57, 7, 18, and 20.
  
  With the mix causing the crash, the maximum observed multicast throughput seen is 170 Mbps, 27.44 Mbps, and 42 Mbps for c3925, c2951, and c1951 respectively. This seems to indicate a multicast performance issue.

  Workaround: There is no workaround.
Caveats for Cisco IOS Release 15.2(2)T

- **CSCts46578**
  Symptoms: Firewall may drop a packet with log similar to:
  ```
  %FW-6-DROP_PKT: Dropping ftp-data session 10.7.7.99:1449 10.7.8.100:20 due to Invalid Seq# with ip ident 6621 tcpflags 0x8018 seq.no 3558493868 ack 1386495675
  ```
  Retransmitted packet is allowed through.
  Conditions: CBAC configured.
  Workaround: There is no workaround.

- **CSCts68626**
  Symptoms: PPPoE discovery packets causes packet drop.
  Conditions: The symptom is observed when you bring up a PPPoE session and then clear the session.
  Workaround: There is no workaround.

- **CSCts69534**
  Symptoms: A Cisco 3800 router running voice debugs may crash with a bus error.
  Conditions: Voice debugs seem to be triggering the crashes.
  Workaround: There is no workaround.

- **CSCts85251**
  Symptoms: Router with GETVPN enabled may experience high CPU and memory exhaustion leading to a crash.
  Conditions: First seen on Cisco IOS Release 12.4(24)T5 but not exclusive to it.
  Workaround: There is no workaround.

- **CSCtt11210**
  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.
  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.
  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.
  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- **CSCtt20719**
  Symptoms: Incremental leaks at shdsl_efmEndpointCurrEntry_get and shdsl_efmInventoryEntry_get.
  Conditions: The symptom is observed with an SNMP walk on a Cisco 888E router and with a Cisco ISR-G2 with HWIC-2SHDSL-EFM.
  Workaround: There is no workaround.

- **CSCtt21228**
  Symptoms: Router crashes while trying to configure Tcl script via SSH connection.
  Conditions: SSH to the router and then try to configure Tcl script.
  Workaround: There is no workaround.
• CSCtt26721
  Symptoms: A Cisco router may see increased CPU utilization when NBAR is used.
  Conditions: This has been experienced on a Cisco 3925 router running Cisco IOS Release 15.1(3)T2.
  Workaround: There is no workaround.

• CSCtt28764
  Symptoms: Throughput and connection rate are degraded by 50%.
  Conditions: This symptom is seen when static ip-sgt bindings are configured on Cisco ISR G2 routers.
  Workaround: There is no workaround.

• CSCtt96462
  Symptoms: Traffic gets dropped across the tunnel interface when you have the following features enabled:
  – NAT
  – VRF
  – IPSec
  Conditions: The symptom is observed when crypto map and VRF are applied under physical interface.
  Workaround: Disable CEF.

• CSCtu08373
  Symptoms: Router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.
  Conditions: IOS firewall is configured and traffic is flowing through the router.
  Workaround: There is no workaround.

• CSCtu11140
  Symptoms: When there is no reachability cache on a DLSw router, the DLSw router sends CUR_EX unexpectedly if receiving XID_F.
  Conditions: The symptom is observed if a DLSw router receives XID_F when there is no reachability cache.
  Workaround: There is no workaround.

• CSCtu16433
  Symptoms: A Cisco 3725 running Cisco IOS Release 12.4(15)T may crash in GETVPN with a bus error. It appears to crash just after registration:
  `%GDOI-5-GM_REGS_COMPL: Registration to KS <snip> complete for group <snip> using address <snip>`
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = <snip>
  Conditions: The symptom is observed on Cisco IOS Release 12.4(15)T14.
  Workaround: There is no workaround.

• CSCtu18634
  Symptoms: ISR G2 fails to relay specific T30 messages in the POTS->IP direction. This would be a dropped DCS/TCF for an inbound fax, or a dropped DIS/CFR for an outbound fax.
Caveats

This will cause fax failure reproducible almost every time from/to specific sources where there is minimal dB loss in the PSTN. It is also commonly seen in PSTN hair-pinning scenarios.

Conditions: The symptom is observed with fax calls through a fax gateway configured for T.38 and running Cisco IOS Release 15.1(3)T2 or higher. The issue is seen when the input signal amplitude is too strong. It can be identified by obtaining a PCM capture and a packet capture and comparing the T30 data. The inbound stream of the PCM capture will show the T30 message, but the packet capture will not.

Workaround: Any one of the following workarounds apply:

- Applying BOTH an input gain of -6 dB and an output attenuation of 6 dB to the voice-port. Note that this will cause audio conversations through the circuit to be 6dB quieter in each direction as well.
- Downgrade to Cisco IOS Release 15.1(3)T1 or earlier.
- Convert to fax/modem passthrough.

- CSCtu21967
  Symptoms: A router configured to be an IP voice gateway may crash.
  Conditions: The exact conditions for this crash are currently unknown.
  Workaround: There is no workaround.

- CSCtu24740
  Symptoms: A Cisco ISR router may unexpectedly reload due to bus error or Segv Exception or experience a spurious access.
  Conditions: The symptom is observed when NAT and dampening are configured on the same interface while the device is running Cisco IOS Release 15.2(1)T or a later release.
  Workaround 1: Remove dampening from the configuration.
  Workaround 2: Downgrade to Cisco IOS Release 15.1(4)M or earlier release.

Resolved Caveats—Cisco IOS Release 15.2(2)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(2)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsh39289
  Symptoms: A router may crash under a certain specific set of events.
  Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.
  Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCso41274
  Symptoms: A router crashes or shows the following traceback:

  % Not enough DSP resources available to configure ds0-group 1 on controller T1 1/0 %
  The remaining dsp resources are enough for 14 time slots. % For current codec complexity, 1 extra dsp(s) are required to create this voice port.
  sip-cme(config-controller)# %ALIGN-3-SPURIOUS: Spurious memory access made at
  0x40C627A8 reading 0x4 %ALIGN-3-TRACE: -Traceback= 0x40C627A8 0x40D6769C 0x40D7281C
  0x40D72E74 0x4036B0E4 0x4036D4B4 0x414C78EC 0x414EB3FC
Conditions: The symptom is observed on a router that has enough DSP resources to set up 14 signaling channels. When trying to configure a ds0-group for the 16 time-slot, you may get an error message that not enough DSP resources are available. Immediately after that the router shows the traceback or may crash.

Example:
```
sip-cme(config)#controller t1 1/0
sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-imm
sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-immediate-start
```
Workaround: Ensure there are more DSPs in the router than signalling channels.

- CSCs046409
  Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.
  Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM-VPN/SSL-3.
  Workaround: There is no workaround.

- CSCsx64858
  Symptoms: A router may crash after the `show ip cef vrf VRF platform` command is issued.
  Conditions: This symptom occurs when BGP routes are learned via two equal paths within a VRF. If an update occurs so that only one path remains while the `show ip cef vrf VRF platform` command is issued, the router may crash.
  Workaround: There is no workaround.

- CSCsz79652
  Symptoms: A memory leak may be seen in Dead memory.
  Conditions: This symptom is observed in Cisco IOS Release 12.2(50)SE and Release 12.2(50)SE1. Cisco IOS Release 12.2(44)SE is not affected. The symptom occurs when using Cisco Network Assistant to poll the device. The `ip http server` command or `ip http secure-server` command must be enabled for the leak to occur.
  Workaround: Disable the http server or stop CNA from polling the device.

- CSCsz97091
  Symptoms: Packet drop occurs when `show version`, `show run`, and `write memory` commands are issued.
  Conditions: Packet drop will be observed as input errors accounted as overruns. The rate of packets being dropped will be proportional to the rate of traffic.
  Workaround: There is no workaround.

- CSCta79941
  Symptoms: A virtual interface is not created when invoked using the `ip unnumbered type number` command.
  Conditions: This symptom is observed under a PPP interface when the virtual interface has been previously deleted.
  Workaround: Recreate the virtual interface manually using the `interface` command.

- CSCta93316
  Symptoms: Memory leaks are seen.
  Conditions: The symptom is observed after the coop functionality test when using the `show memory debug incremental leaks` command.
  Workaround: There is no workaround.
- **CSCtb24819**
  Symptoms: CLI view created cannot be deleted when user logs in and out. View deletion fails when user first sets into a view and then moves to another view or root view and tries to delete the previously set view.

  Conditions: This issue occurs when a view user telnets into the device and then switches to another view or to root view. This is seen consistently when a view is created and user logs in as a view user.

  Workaround: Log in as the root view user first and then delete the view.

  Further Problem Description: This issue only affects those view users who would log in as a view user and then tries to delete the view by changing itself to another view or the root view.

- **CSCtb57180**
  Symptoms: A router may crash with a software-forced crash.

  Conditions: Under certain conditions, multiple parallel executions of the `show users` command will cause the device to reload.

  Workaround: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet, and SSH.


  The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

  ```
  Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
  Router(config)# access-list 1 permit host 172.16.1.2
  Router(config)# line vty 0 4
  Router(config-line)# access-class 1 in
  ```

  For devices that act as a terminal server, to apply the access class to reverse telnet ports, the access list must be configured for the aux port and terminal lines as well:

  ```
  Router(config)# line 1 <x>
  Router(config-line)# access-class 1 in
  ```

  Different Cisco platforms support different numbers of terminal lines. Check your device’s configuration to determine the correct number of terminal lines for your platform.

  Setting the access list for VTY access can help reduce the occurrences of the issue, but it cannot completely avoid the stale VTY access issue. Besides applying the access list, the following is also suggested:

  1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.
  2. Avoid issuing the `clear vty` command or the `clear line` command when there is any nested VTY access.
  3. Avoid issuing the `clear vty` command or the `clear line` command when there are multiple VTY accesses from the same host.
  4. Avoid issuing the `clear vty` command or the `clear line` command when router CPU utilization is high.
  5. Avoid issuing the `show users` command repetitively in a short period of time.

  Again, the above can help reduce the occurrences of the issue, but it cannot completely avoid the issue.
- **CSCtb69063**
  Symptoms: Memory corruption occurs when a user name is configured to a maximum length of 64 characters, as shown:
  ```
  config# username <name of 64 characters> priv <0-15> password 0 <password>
  ```
  Conditions: The symptom is observed if the user name is exactly 64 characters.
  Workaround: Configure a user name of less than 63 characters.
  Further Problem Description: When some configurations are added, modified, or deleted the `show configuration id detail` command prints information of last change time, changed by user, and changed from process. If the user name is very large (exactly 64 characters), then the “changed by user” field prints unwanted characters.

- **CSCtc78200**
  Symptoms: A Cisco router may crash in the `parse_configure_idb_extd_args` routine.
  Conditions: This symptom is observed when running PPP sessions or when TCL is used for configuring interface range.
  Workaround: As PPP session is being established on the LNS, IOS will momentarily use one of the available VTYs from the router. After initial configuration is done, it is immediately released to the system pool.
  If all VTY connections are in use, then we will see an RP crash if a new PPP session is being established and there are no free VTYs in the system.
  To work around this issue, reserve several VTY connections for PPP session establishment. Since it is possible that a burst of PPP sessions tries to connect thereby using multiple VTY connections at the same time, it is recommended to reserve at least 5 VTY connections. One possible solution is to use an ACL on the last 5 VTY lines:
  ```
  ip access-list extended VTY_ACL
  deny ip any any
  
  line vty 5 9
  access-class VTY_ACL in
  exec-timeout 1 0
  ```
  Alternate Workaround: Do not configure “interface range” cli using `ios_config` from tclsh mode. When in tclsh mode, use normal “interface cli” in a “for loop”.

- **CSCtc96631**
  Symptoms: Packet drops occur in downstream devices every 4ms burst from shaper.
  Conditions: The symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.
  Workaround: Use ASRs instead of ISR.

- **CSCtd15853**
  Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.
  Conditions:
  - mVPN is configured on the PE router.
  - Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.
  Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier:
Caveats


Workaround: There is no workaround.

- CSCt70365
  Symptoms: When “config ED” is used for EEM with some special configurations (like virtual-template commands), it can trigger error messages.
  Conditions: The symptom is observed only when certain commands are configured.
  Workaround: Use “syslog ED”.

- CSCtg35257
  Symptoms: The message “previous instance of CNS Event Agent still executing” is seen even if a CNS event is not configured.
  Conditions: The symptom is observed if the `cns event <IP> encrypt` command is enabled and disabled.
  Workaround: There is no workaround.

- CSCth06812
  Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.
  Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1. (XNE1) and the following configuration:
  ```
  R1(config)#parser view SUPPORT
  R1(config-view)# secret cisco
  R1(config-view)# commands exec include ping
  R1(config-view)# commands exec include configure terminal
  R1(config-view)# commands exec include show ip ospf neighbor       <--Where we see the hang
  ```
  Workaround: Do not configure “commands exec include show ip ospf neighbor” command in parser view configuration.

- CSCth07787
  Symptoms: A standby device crashes when attempting to configure login banner on the active device.
  Conditions: The symptom is observed only when configuring the banner manually, but not during bulk sync or any copy operations. In addition, this symptom is observed when using the following delimiters: -Cntrl-v + Cntrl-C -Shift-6 + Shift-C
  Workaround: Use any delimiters other than the following: -Cntrl-v + Cntrl-C -Shift-6 + Shift-C.

- CSCth11006
  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:
  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol
  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.
  Cisco has released free software updates that address these vulnerabilities. This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat
• CSCth80642
Symptoms: IOS SSLVPN fails to accept new ssl connection. Sessions get stuck in Time Wait until TCP queue is full.
Conditions: SSLVPN on IOS
Workaround: clear tcp tcb * will clear Time Wait sessions

• CSCth82293
Symptoms: ISR-G2 router crashes due to bus error at PC 0x0 with spurious errors and the following message:
%ALIGN-1-FATAL: Corrupted program counter
Conditions: The symptom is observed with wrong usage of CNS initial and partial configurations mixed with cns config retrieve execution.
Workaround: Avoid wrong CNS usage. Consult Cisco for correct CNS usage.
Further Problem Description: Although the issue is seen with a Cisco 2911, it is not specific to the 2900 series alone. It can occur with any router platform.

• CSCth83508
Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.
Conditions: The problem is seen when using WSMA to run the session install command.
Workaround: Perform the install manually from a VTY session.

• CSCti13493
Symptoms: A router crashes and the following traceback is seen:
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 47523D58. - Process= "DSMP",
ipl= 0, pid= 226, -Traceback=
TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x430853EC
Conditions: The symptom is observed with the DSMP process.
Workaround: There is no workaround.

• CSCti24577
Symptoms: System crashes on active or hangs on standby.
Conditions: The symptom is observed when a banner command is in the configuration.
Workaround: Remove all banner commands.

• CSCti33159
Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed to using the directly-connected link.
Conditions: This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor and the other interface is one hop away.
Workaround: There is no workaround.

• CSCti66155
Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.
Caveats

Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- CSCti67832
  Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.
  Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug `debug crypto gdoi gm all-features`.
  Workaround: There is no workaround.

- CSCti68721
  Symptoms: The output of `show performance monitor history interval <all | given #>` will appear to have an extra column part way through the output.
  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.
  Workaround: If the symptom occurs, repeat the command.

- CSCti92798
  Symptoms: A Cisco router crashes while configuring http commands with ATM.
  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(2)T.
  Workaround: There is no workaround.

- CSCtj05903
  Symptoms: Some virtual access interfaces are not created for VT, on reload.
  Conditions: This symptom occurs on scaled sessions.
  Workaround: There is no workaround.

- CSCtj06390
  Symptoms: Ping fails after configuring crypto.
  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.18)T.
  Workaround: There is no workaround.

- CSCtj10592
  Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.
  Conditions: The symptom is observed with a simple SVTI to DVTI connection.
  Workaround: There is no workaround.
- **CSCtj21237**
  Symptoms: %SYS-2-LINKED: Bad enqueue, Bad dequeue messages are received, which might result an in unexpected reboot due to SegV Exception.
  Conditions: The symptom is observed on a router configured with control plane policing and protection feature.
  Workaround: Disable the feature in order to prevent any further crash.

- **CSCtj38234**
  Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.
  An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.
  Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).
  Workaround: There is no workaround.

- **CSCtj47822**
  Symptoms: The standby RP is stuck in standby_issu_negotiation_late state after a switchover and does not come to SSO. Also, memory leaks are seen at tid_cmn_add_or_find_port_info.
  Conditions: The issue occurs during the peer (standby RP) reset or switch- over.
  Workaround: There is no workaround.

- **CSCtj56551**
  Symptoms: The Cisco 7600 crashes in a very rare case.
  Conditions: This symptom is observed very rarely when route-churn/sessions come up.
  Workaround: There is no workaround.

- **CSCtj69212**
  Symptoms: High level of memory usage due to “MAB Framework” process.
  Conditions: This issue is seen on Cisco Catalyst 3750 switches running Cisco IOS Release 12.2(55)SE when MAB fails on the port and subsequent attempts are made to authorize the device after the restart timer expires.
  Workaround: Unconfigure the following from the switch:
  ```
  aaa accounting send stop-record authentication failure
  ```

- **CSCtj76297**
  Symptoms: Router hangs with interoperability of VM and crypto configurations.
  Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.
  Workaround: Disable AIM and use onboard CE.

- **CSCtj78966**
  Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.
  Conditions: This symptom is seen when IKEv2 SA DB WAVL tree is getting corrupted if we fail to insert the SA due to some error, for example, PSH duplication.
Workaround: There is no workaround.

- CSCtj79368
  Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.
  Conditions: The symptom is observed when removing RSA keys.
  Workaround: Stay on the same RSA keys.

- CSCtj95685
  Symptoms: A router configured as a Voice Gateway may crash while processing calls.
  Conditions: The symptom is observed with a router configured as a Voice Gateway.
  Workaround: There is no workaround.

- CSCtk00181
  Symptoms: Password aging with crypto configuration fails.
  Conditions: The symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.
  Workaround: There is no workaround.

- CSCtk13560
  Symptoms: xauth userid mode http-intercept does not prompt for a password and the EzVPN session does not come up.
  Conditions: This symptom occurs when the EzVPN client, x-auth is configured as http-intercept.
  Workaround: There is no workaround.

- CSCtk18404
  Symptoms: Per-user route is not installed after IPCP renegotiation.
  Conditions: The symptom is observed with the following conditions:
  1. PPP session comes up, NAS installs static routes which are sent as attribute from RADIUS server.
  2. After a while, if CPE asks for IPCP renegotiation, IPCP is renegotiated but the static routes are lost.
  Workaround: There is no workaround.

- CSCtk59012
  Symptoms: After PRE switchover, the new standby PRE goes in “progress to standby cold-bulk” state and is then periodically reset by the new active PRE.
  Conditions: This issue is observed when a Cisco uBR10K is configured with 300k routes and a PRE switchover occurs.
  Workaround: There is no workaround.

- CSCtk69114
  Symptoms: RP resets while doing ESP reload with crypto configuration.
  Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.
  Workaround: There is no workaround.
- CSCtk98248
  Symptoms: An FA8 line protocol goes down after the connected device is reloaded.
  Conditions: The symptom is observed with the only FA8 port.
  Workaround: Set the FA8 to auto negotiation.

- CSCtl01141
  Symptoms: cswmMvrfStatsTable does not get populated.
  Conditions: This symptom occurs when the multicast vrf instance is configured on any switch running mtrose image and mibwalk is configured on cswmMvrfStatsTable.
  Workaround: There is no workaround.

- CSCtl20993
  Symptoms: Router crashes during IPsec rekey.
  Conditions: The conditions for this crash are currently unknown.
  Workaround: There is no workaround.

- CSCtl23748
  Symptoms: EoMPLS over GRE (DMVPN) with IPSec protection is not working after a reboot.
  Conditions: The symptom is observed when there is a tunnel (Ethernet over MPLS over GRE over IPsec) between PE1 and PE2 and following a reload and when tunnel protection is configured.
  Workaround: There is no workaround.

- CSCtl48297
  Symptoms: Configure BGP dynamic neighbor in IPv4 VRF address-family. Deconfiguring BGP by using the `no router bgp` command will crash the system.
  Conditions: This symptom occurs because BGP dynamic neighbor feature currently is not supported but is allowed to be entered in CLI.
  Workaround: Do not configure BGP dynamic neighbor in VRF address-family.

- CSCtl49844
  Symptoms: Carrier delay configured under interface fails.
  Conditions: The symptom is observed when the cable is detached.
  Workaround: There is no workaround.

- CSCtl50815
  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:
  
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason Non-OER, OOP Reason <reason>
  
  Conditions: The symptom is observed under the following conditions:
  - Use ECMP.
  - Use `mode monitor passive`.
  
  Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.
Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl52854
  Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.
  Conditions: The symptom is observed when a multicast server is connected to an EHWIC L2 interface.
  Workaround: Connect the multicast server to an on-board gig interface.

- CSCtl54975
  Symptoms: A small number of Cisco 1812 routers have been observed to unexpectedly restart due to software-forced crashes, repeatedly.
  Conditions: Unknown.
  Workaround: While the root cause is being investigated, units that are experiencing this problem should be replaced. Please replace the Cisco 1812 and send the unit for Failure Analysis, after contacting the Cisco TAC and referencing this bug ID.

- CSCtl55502
  Symptoms: Any parser command with a pipe option used in an HTTP URL is not working properly and giving the help option instead of the actual output.
  Conditions: The symptom is observed when a parser command uses a pipe option in an HTTP URL (e.g.: http://<ipaddr>/level/15/exec/show/runn/|/i/http/CR).
  Workaround: There is no workaround.

- CSCtl58005
  Symptoms: Accounting delay start is sent before any NCP has been negotiated, with “aaa accounting delay-start” configured. According to PRD, accounting start should not be sent until first NCP has been negotiated.
  Conditions: This symptom occurs when “aaa accounting delay-start” is configured.
  Workaround: There is no workaround.

- CSCtl76050
  Symptom: Traceback is observed.
  Conditions: This symptom is seen while defaulting the call-home profile.
  Workaround: There is no workaround.

- CSCtl76209
  Symptoms: Standby reloads when dampening is configured.
  Conditions: This symptom occurs when dampening is configuring parameters that are within the allowed range but the leading maximum penalty is bigger than the allowed maximum (20000). The RP and standby get out of sync. The command is accepted on active RP first, and standby also accepts it. However, then on active and standby, dampening gets turned off because later it is realized that maximum penalty is higher than 20000. When dampening gets configured again at this point, standby may turn dampening off while the active has it enabled, which will lead to configuration mismatch between active and standby, and standby will reload.
  This can be seen with all address families.
Workaround: There is no workaround.

- **CSCtl82255**
  
  **Symptom:** The following is seen on the UUT when the peering IPv6 router does a session reset.

  ```
  ios72ta2-1#show bgp ipv6 unicast summary
  BGP router identifier 10.0.0.0, local AS number 1
  BGP table version is 34, main routing table version 34
  >>> ....
  Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
  State/PfxRcd
  2011::1001      4            1      22      27       32    0    0 00:19:44 0
  >>>>>>> Table version is different from the main table version ....
  Conditions: This symptom occurs when the peering IPv6 router does a session reset then the “show bgp ipv6 unicast summary” does not get to a state where the main table version matches the peers table version. There is no prefix left behind unadvertised.
  Workaround: Hard clear the router that shows mismatch in table version.
  ```

- **CSCtl87463**
  
  **Symptoms:** Queue length becomes negative.
  
  **Conditions:** The symptom is observed when Cisco IOS-WAAS is configured on the interface.
  
  Workaround: There is no workaround.

- **CSCtl90292**
  
  **Symptoms:** The following error messages are displayed: an 18 08:00:16.577 MET:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes failed from 0x42446470, alignment 32 Pool: I/O Free: 11331600 Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "BGP I/O", ip= 0, pid= 564 -Traceback= 417EB8EC 4180FA6C 42446478 42446B64 42443984 40FC18C8 40FCCB4C 40FD1964 403BDBFC 403BCC34 40344508 403668AC
  Conditions: This symptom is observed when several hits and failures are seen for medium buffers. All are linktype IPC. For example:
  ```
  ```
  Buffer information for Medium buffer at 0x4660E964 ... linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0 if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)
  Workaround: There is no workaround.
  ```

- **CSCtl95666**
  
  **Symptoms:** Data path fails after SSO.
  
  **Conditions:** This symptom is seen when connection segments are down in standby for auto-provisioned VCs.
  
  Workaround: There is no workaround.

- **CSCtn02632**
  
  **Symptoms:** A MAB supplicant never gets authenticated and remains in RUNNING state.
  
  **Conditions:** This symptom is observed when a MAB supplicant connected to FA1 port of a Cisco 890 router remains in RUNNING state indefinitely after issuing a warm reload of router.
  
  Workaround: Use other FE ports if a warm reload is issued.

- **CSCtn04357**
  
  **Symptoms:** When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:
Caveats for Cisco IOS Release 15.2(2)T

Caveats

vlan configuration 161
ip flow monitor flowmonitor1 in
ip flow monitor flowmonitor1 input

Conditions: The symptom is observed on a Sup7-E that is running Cisco OS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

Workaround 1: Remove the flow monitor configuration.
Workaround 2: Use netflow-v9 export protocol.
Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn04716
Symptoms: Upon switchover, standby reloads continuously because of configuration sync failures for OSPF area commands under non-base topologies.
Conditions: This symptom occurs under the following steps:
1. An area X needs to be first configured under base topology.
2. One or more area commands under non-base topology should be configured for area X.
3. All area commands for area X under base topology are removed such that the command(s) under non-base topologies are the only ones that remain. Note that this cannot be achieved for area X stub, area X nssa, and area X virtual-link commands as removal of these commands under base topology will result in removal of corresponding commands under non-base topologies as well.
4. Execute switchover.
Workaround: Remove the commands under non-base topologies before switchover.

- CSCtn21501
Symptoms: A Cisco 2900 series router with switch modules (such as HWIC-4ESW-POE) does not respond to SNMP queries on the BRIDGE-MIB.
Conditions: The symptom is observed on a Cisco 2900 series router (with switch modules) that is running Cisco IOS Release 15.x.
Workaround: There is no workaround.

Further Problem Description: This issue is similar to CSCsb46470.

- CSCtn22728
Symptoms: See the following:
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#destination ?
<cr>
Router(config-mon-erspan-src)#destination int g11/48
Router(config-if)#
Config Sync: Line-by-Line sync verifying failure on command:
   destination int g11/48
due to parser return error
Conditions: This symptom is seen when using unsupported interface CLI option with destination keyword in ERSSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.
Workaround: Do not issue not applicable commands.
- **CSCtn22930**
  Symptoms: PLATFORM_VALUE_EIGRP_TRACE_LOG_SIZE_IN_KB should not be hard coded to 20. The PLATFORM_VALUE_CRASH_BUFFER_SIZE is already defined as 20.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCtn24305**
  Symptoms: The software version in call home messages has a trailing comma for the released images. This causes a backend processing failure when the software version is needed.
  Conditions: All call home messages from released images have this issue.
  Workaround: Backend can check to remove this trailing comma, if present.

- **CSCtn26750**
  Symptoms: The standby RP reloads due to a config-sync error.
  Conditions: The symptom is observed when “authentication” or “encryption” is configured for an OSPFv3 virtual link. Then it is changed to use a different SPI, but IPSec fails to remove the policy for the old SPI. When it is changed back to the old SPI, the command fails with the error:
  %OSPFv3-3-IPSEC_POLICY_ALREADY_EXIST: SPI is already in use with ospf process
  On the active RP the “virtual-link ipsec” configuration is removed, but on the standby RP it remains. Reconfigure “virtual-link ipsec” using the second SPI. This command succeeds on the active RP so it is synched to the standby, however the command already exists on the standby so it generates the config-sync error and reloads.
  Workaround: Instead of simply changing the SPI from X to Y, remove X using a no command and then configure Y.

- **CSCtn32323**
  Symptoms: 802.1p information is not set on local generated traffic when bridge-dot1q is used on the DSL lines.
  Conditions: Configure the device to transport 802.1p information over a DSL link connection, considering different CoS values for LAN and local generated traffic on the router.
  ```
  interface ATM0.y point-to-point
  bridge-group <x>
  pvc 1/199
  bridge-dot1q encap <vlan>
  service-policy out <egress-policy>
  ```
  Workaround: There is no workaround.

- **CSCtn39339**
  Symptoms: Data path fails with Hot-Standby Psuedo Wire (HSPW) configurations after a switchover.
  Conditions: The symptom is observed when a switchover occurs with the backup pseudowire up and the primary pseudowire down.
  Workaround: There is no workaround.

- **CSCtn39632**
  Symptoms: RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.
  Conditions: This occurs on a Cisco ASR 1000 series router configured for RSA key encryption with a keyring name having more than 8 characters.
• CSCtn39950
Symptoms: An IPsec session will not come up.
Conditions: This symptom occurs if a Cisco ISR G2 has an ISM VPN accelerator and slow interfaces such as BRI-PRI. Crypto plus ISM VPN module plus slow interfaces will not work.
Workaround: Disable the ISM VPN module and switch to the onboard crypto engine.

• CSCtn40571
Symptoms: Issuing the `crypto pki server name rollover cancel` command can result in multiple rollover certificates installed on Sub-CA router.
Conditions: This symptom is seen when the rollover certificate is already installed.
Workaround:
- Copy startup-configuration from router.
- Remove the older rollover certificate from configuration under the `crypto pki cert chain ca` command.
- Copy the new configuration back to startup-configuration and reload the router.

• CSCtn42588
Symptoms: After seeing OSPF neighbors flap quickly one of the neighbors does not properly install routes that should be learned via OSPF. The routes may appear in the OSPF LSDB.
Conditions: The symptom is observed when “timers throttle spf” or “timers throttle lsa” is configured.
Workaround: Use default SPF or LSA timers or ensure your LSA timers are smaller than the SPF timers.

• CSCtn43589
Symptoms: A crash is observed at `process_run_degraded_or_crash`.
Conditions: The symptom is observed when SNMP bulkstat has been configured for periodic MIB collection.
Workaround: There is no workaround.

• CSCtn53730
Symptom: A device running Cisco IOS Release 15.1(3)T with NAT may reset due to a bus error when passing certain DNS over TCP packets.
System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xDDDDDDDD
Conditions: NAT must be enabled, and only certain DNS over TCP packets can trigger the issue.
Workaround: There is no known workaround.
Further Problem Description: DNS over TCP is a requirement for a full DNS implementation

• CSCtn56097
Symptoms: Auto mpls-lsp-monitor for pathecho fails.
Conditions: Auto mpls-lsp-monitor feature does not work due to internal scheduling error.
Workaround: There is no workaround.

• CSCtn58005
Symptoms: The prefix-list does not filter local routes configured in the L1-L2 domain.
Conditions: The symptom is observed on a router running IPv6 ISIS L1-L2 domain and when L1 routes are redistributed into L2 routes.
Workaround: There is no workaround.

- CSCtn58128
  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.
  Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.
  Workaround: Ensure “no logging console” is configured.

- CSCtn59075
  Symptoms: A router may crash.
  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible Netflow needs to be running.
  Workaround: There is no workaround.

- CSCtn62287
  Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.
  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.
  Workaround: There is no workaround.

- CSCtn65116
  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.
  Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Release 12.2(33)SRB and later. Earlier versions are not affected.
  Workaround: Advertise and withdraw or withdraw and re-advertise a more specific prefix. That will force the re-evaluation of the prefix not being imported, for import again.

- CSCtn67577
  Symptoms: SIP-400 crashes while modifying the cell-packing values.
  Conditions: This symptom occurs when cell-packing values are modified at PE2 side.
  Workaround: There is no workaround.

- CSCtn68117
  Symptoms: Session command does not work on Cisco C3K series routers that have become the master after a mastership change.
  Conditions: This symptom is seen when fail-over to slave occurs.
  Workaround: There is no workaround.

- CSCtn70367
  Symptoms: IPSEC key engine crashes at sessions setup.
Conditions: This symptom is seen when setting up sessions with the configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. The crash happens on IPSEC key engine. The crash occurs while UUT is establishing SAs that are requested. This issue is reproduced by clear crypto session on CES after all SAs are established.

Workaround: There is no workaround.

- CSCn72925
  Symptoms: PFR fails to get notified about interface state changes.
  Conditions: The issue is seen specifically when using Frame Relay and Multilink Frame Relay subinterfaces as PFR external exit and the main interface flaps.
  Workaround: Use the following command:
  `clear pfr master *`.

- CSCn88247
  Symptoms: The command `no ip address` is not NVgened on the interface if the switchport configuration is removed from the interface after a reload.
  Conditions: The symptom is observed if you reload the router having one or more interfaces configured with switchport and you then remove the configuration after the reload.
  Workaround: There is no workaround.

- CSCn97267
  Symptoms: There is a router crash in the URLF code using Websense.
  Conditions: The symptom is observed on a Cisco ISR G2 during normal operation. It is caused by long URLs overwriting the end of a fixed length buffer.
  Workaround: There is no workaround.

- CSCto08135
  Symptoms: When a deny statement is added as the first ACL, the message gets dropped.
  Conditions: An ACL with deny as the first entry causes traffic to get encrypted and denied.
  Workaround: Turn off the VSA, and go back to software encryption.

- CSCto09059
  Symptoms: CPUHOG at IPC Check Queue Time Process results in IOSD crash.
  Conditions: This symptom occurs with multiple RP switchovers with ISG PPPoE sessions.
  Workaround: There is no workaround.

- CSCto10485
  Symptoms: With a GRE over IPSec configuration using tunnel protection, traffic originated from the router may be dropped on the receiving router due to replay check failures. This is evident by the `%CRYPUO-4-PKT-REPLAY` drops as shown in the syslog.
  Conditions: This issue typically occurs during high traffic load conditions.
  Workaround: There is no workaround.

- CSCto11238
  Symptoms: OSPF cannot be enabled on a tunnel interface by using either the network statement under OSPF or by enabling OSPF directly under the interface.
  
  Router#show ip osp neighbor tunXXX
  %OSPF: OSPF not enabled on TunnelXXX
Conditions: This symptom is observed in both Cisco IOS Release 15.1S and Cisco IOS Release 15.1T IOS software trains. The problem is triggered by configuring either WCCP, L3VPN, or mGRE. A tunnel configured with any of these will have dynamic routing disabled on it. If this is then deleted, the idb is reused by a new tunnel created via the CLI. This newly created tunnel will still have dynamic routing disabled on it and therefore ospf cannot run on it.

Workaround: Once the problem has occurred, the only way to recover is to reload the router. If WCCP, L3VPN, or mGRE are never configured, the issue will not be seen.

- CSCto13338
  Symptoms: When a PSTN phone is calling an IP Phone that is forwarded to a PSTN destination, the call is placed but no audio is present. This is the same behavior with blind transfer to external destinations.
  Conditions: This symptom occurs when voice-class codec X offer all and transcoders are used with CUBE.
  Workaround 1: Use the codec XXXX command instead of voice-class codec X offer all.
  Workaround 2: Use consultative transfer instead of blind transfer.

- CSCto15361
  Symptoms: MF: Active Supervisor crashes after removing the "router eigrp" configuration.
  Conditions: This symptom occurs when the Active Supervisor crashes while disabling the Ipv6 router eigrp because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.
  Workaround: Modify the igrp2_procinfo_free function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto16196
  Symptoms: Performing a no wccp version2 on the WAAS device connected to the WAN link and then reconfiguring wccp version 2 results in tracebacks on a Cisco ASR 1000 router configured with WCCP. Traffic loss is also observed.
  Conditions: This symptom is observed when WCCP is configured on a Cisco ASR 1000 router and the WCCP tunnels are up before wccp version 2 is removed and reapplied on the WAAS devices.
  Workaround: There is no workaround.

- CSCto31255
  Symptoms: Router crashes at fair-enqueue.
  Conditions: The symptom may be seen on Cisco 5400 and 7200 platforms.
  Workaround: There is no workaround.

- CSCto34844
  Symptoms: The Cisco 891 may perform lower than the older generation Cisco 1812 platform.
  Conditions: This symptom occurs when Ethernet traffic using the VLAN tag is encapsulated inside the L2TPv3 tunnel.
  Workaround: There is no workaround.
- **CSCto39885**
  Symptoms: A router crashes.
  Conditions: gcid and callmon is turned on.
  Workaround: There is no workaround.

- **CSCto41215**
  Symptoms: DHCP server tries to assign a conflicted address to a client when “remembered binding” is configured.
  Conditions: The symptom is observed when the remember keyword is configured in the server pool and the address that the server is going to assign is already assigned to another client.
  Workaround: Ensure each client in the network is configured or gets a unique IP address.

- **CSCto42752**
  Symptoms: Removing the existing static policy and applying it back or adding the policy under that interface if it does not exist results in an error on standby.
  Conditions: This symptom occurs when customers use high availability.
  Workaround: Using the non-HA or standalone routine will fix the problem.

- **CSCto48060**
  Symptoms: A Cisco 3900 series router may crash with the following error:
  Unexpected exception to CPU: vector 1400
  Conditions: The symptom is observed when the router is configured as a voice gateway using H323 and H245 and connected to CUCM. If CUCM is sending a MultiMediaSystemControl messages with no entry, the router may crash.
  Workaround: There is no workaround.

- **CSCto55606**
  Symptoms: When same remote unicast neighbor is configured and received on different interfaces, the two neighbors keep flapping.
  Conditions: This symptom is seen when the same EIGRP neighbor is coming up on different interfaces.
  Workaround: This may not be a recommended configuration since having the same neighbor on different interfaces is not allowed in classic mode. This option is provided only for certain migration scenarios.

- **CSCto60216**
  Symptoms: Cisco IOS crashes in ospfv3_write.
  Conditions: This symptom occurs when the issu runversion command is entered multiple times within a short period of time.
  Workaround: Wait for the newly active router processor to completely initialize.

- **CSCto61485**
  Symptoms: High CPU utilization is seen after session disconnect.
  Conditions: This symptom is observed with scaling test cases with 10K to 24K sessions.
  Workaround: There is no workaround.
• CSCto61736
  Symptoms:
  1. NBAR remains enabled in CEF path.
  2. Packet counters not incrementing in “show adjacency lisp0 detail”.
  3. ADQ/PD not working on ATM-subinterface and frame-relay subinterfaces.
  4. `ip nbar port-map` CLI is broken.
  Conditions:
  1. The symptoms 1 and 2 are observed when NBAR is enabled and disabled on the interface.
  2. Symptoms 3 and 4 are seen when the configuration/show CLIs are executed.
  Workaround: There is no workaround.

• CSCto63268
  Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.
  Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.
  Workaround: Remove the EVM or disable DSP sharing.

• CSCto76700
  Symptoms: Multihop BFD session goes down with TE-FRR cutover.
  Conditions: The symptom may be observed with single hop, VCCV BFD and multihop BFD sessions. But after the TE-FRR cutover, the VCCV BF session comes back up whereas multihop BFD session goes down.
  Workaround: The workaround is to perform a “no shut” the port-channel interface.

• CSCto76888
  Symptoms: G.729 payload issue on a Cisco 2800. A PSTN user calls up on a specific number which is directed to the IVR response via the Cisco 2800 gateway router, but the PSTN user cannot hear anything due to the codec payload mismatch.
  Conditions: The symptom is observed with a first preference of the Codec G.729ab which is sent to a Cisco 2851 for an IVR announcement.
  Workaround: Change the preference of the Codecs to have G.729a as the preferred Codec from MGX.

• CSCto77352
  Symptoms: Standby cannot reach HOT sync state with active. Standby RP will keep resetting. The following messages are printed:

  `%SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1), process = IPC Dynamic Cache`

  Conditions: This symptom occurs with SSO mode when a Cisco ASR 1000 series router is configured with ISG as DHCP server and with low DHCP lease timer.
  Workaround: There is no workaround.

• CSCto81701
  Symptoms: The PfR MC and BR sessions flap.
  Conditions: The symptom is observed with a scale of more than 800 learned TCs.
Workaround: Use the following configuration:
```
pfr master keepalive 1000
```

- **CSCto81916**

  Symptoms: Voice gateway crashes due to insufficient free memory.

  Conditions: The symptom is observed when the copy feature is used in a voice class SIP profile similar to the example below:

  ```
  voice class sip-profiles 500
  request INVITE peer-header sip Remote-Party-ID copy ":(.*)@" u01
  request INVITE sip-header From modify "From: "anonymous\" "<\1>"<\2>" <\1>"<\2>"
  !
  ```

  In this case, a memory leak occurs and depletes all the free memory causing the router to crash.

  Workaround: There is no workaround.

- **CSCto85479**

  Symptoms: Spanning Tree Protocol (STP) failure on EHWIC-4ESG.

  Conditions: The symptom is observed on a Cisco 3945 chassis that is running the c3900-universalk9-mz.SPA.151-4.M.bin image. Interfaces gi0/3/0-1 are on EHWIC-4ESG card.

  Workaround: There is no workaround.

- **CSCto85731**

  Symptoms: Crash seen at the nhrp_cache_info_disseminate_internal function while verifying the traffic through FlexVPN spoke-to-spoke channel.

  Conditions: The symptom is observed under the following conditions:

  1. Configure hub and spokes (flexvpn-nhrp-auto connect) as given in the enclosure.
  2. Initiate the ICMP traffic through spoke-to-spoke channel between spoke devices.
  3. Do a clear crypto session at Spoke1.
  4. Repeat steps 2 and 3 a couple of times.

  Workaround: There is no workaround.

  Further Problem Description: In the given conditions, one of the spoke device crashed while sending ICMP traffic (10 packets) through FlexVPN spoke-to-spoke channel. The crash decode points to “nhrp_cache_info_disseminate_internal” function

- **CSCto88393**

  Symptoms: CPU hogs are observed on a master controller:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)ms, more than (2000)ms (0/0),process = OER Master Controller.
  ```

  Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.

  Workaround: There is no workaround.

- **CSCto89536**

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
Caveats for Cisco IOS Release 15.2(2)T

- Memory Leak in H.323 Inspection
- Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

- CSCto90912

Symptoms: A crash is seen with the DHCPv6 client process.
Conditions: The symptom is observed when `ipv6 address dhcp` is run on an “auto-template” interface, and then the interface is removed with a `no int auto-temp`.

Workaround: There is no workaround.

- CSCto92529

Symptoms: Unable to configure “ipv6 ospf authentication ipsec spi 7000 md5 <>”.
Conditions: The symptom is seen on Cisco routers loaded with Cisco IOS interim Release 15.2(2.11)T.

Workaround: There is no workaround.

- CSCto96750

Symptoms: The `shutdown` command does not show up in the active running-config.
Conditions: The following steps recreate the issue:
1. Administratively shutdown a interface.
2. Make this interface as the backup for another interface.
3. Running-config of backup interface in the active does not synch up with standby running-config in SSO mode.

Workaround: There is no workaround.

- CSCto99343

Symptoms: Linecards do not forward packets which causes a failure on the neighborship.
Conditions: The symptom is observed on VSL-enabled linecards on a VSS system.

Workaround: There is no workaround.

- CSCtq05004

Symptoms: A dialer loses its IP address sporadically. The `show interface atm x` will record output drops during the issue. ATMO is up, line protocol is up:

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 31956 << Incrementing during the issue
```

The `show interface queueing atm0.1` (hidden command) will show as follows:

```
Interface ATM0 VC 8/35
Queueing strategy: fifo
Output queue 40/40, 31956 drops per VC << Incrementing during the issue
```

During the issue, if “debug ppp negotiation” is on, we will see the following:

```
PPP: Missed 5 keepalives, taking LCP down
PPP DISC: Missed too many keepalives
```

There will be no ATM (physical interface) flap in this case (during the issue).

A shut/no shut on the ATM interface does not help.
Caveats

Conditions: No conditions so far. The behavior is sporadic.
Workaround: Reload.

- **CSCtq06105**
  Symptoms: In an MPLS FRR setup, after shut and unshut of the primary interface, traffic continues to flow along the backup interface, which is wrong. Traffic should flow along the primary path once the primary path is restored.
  Conditions: This symptom occurs with a MPLS FRR setup. The primary interface should be shut and unshut to see the issue.
  Workaround: Shut and unshut the backup interface. This will make traffic flow along the primary path again, and also get the backup path in ready state.

- **CSCtq10684**
  Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.
  Conditions: This symptom occurs when tunnel flap is observed before the crash.
  Workaround: A possible workaround is to reload the box.

- **CSCtq17082**
  Symptoms: Router reloads.
  Conditions: The symptom is observed with at least 2000 IPSec tunnel sessions by automatic script to remove a QoS configuration from Virtual Template.
  Workaround: Session teardown before you remove the QoS configuration.

- **CSCtq21234**
  Symptoms: Label is not freed.
  Conditions: The symptom is observed after shutting down the link.
  Workaround: There is no workaround.

- **CSCtq21785**
  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(2)S may crash upon performing a CRL check on an invalid certificate.
  Conditions: The conditions are unknown.
  Workaround: Turning off CRL check should stop the crash. It should be configured as: "revocation-check none"
  This will stop the CRL check of the peer certificate but should not be a long term solution.

- **CSCtq24006**
  Symptoms: DMVPN tunnels will not come up with an IPv6 address.
  Conditions: This symptom is observed if more than one tunnel is present on the spoke.
  Workaround: There is no workaround.

- **CSCtq24614**
  Symptoms: The commands to ignore S1 bytes are not supported on an ATM interface.
  Conditions: The symptom is observed with an ATM SPA.
  Workaround: There is no workaround.
• CSCtq24733
  Symptoms: VXML gateway crash with “Unexpected exception to CPU: vector C”.
  Conditions: The symptom is observed with MRCP is enabled.
  Workaround: There is no workaround.

• CSCtq26863
  Symptoms: After issuing a `shutdown` command on a port or unplugging the port, `show authentication session interface fax/x` will in some occasions show that the session informartion persists.
  This can cause issues if the port was previously authenticated to the auth critical or guest VLAN, as the switch will retain this session information when the port is restarted and will ignore EAPoL requests sent by the dot1x supplicant.
  Conditions: Issue has been observed under the following circumstances:
  – Cisco IOS Release 12.2(33)SXI6 (same environment did not see the issue under an earlier code).
  – Multidomain authentication configured.
  – Issue intermittently reproducible when many ports are brought online at the same time.
  The issue is due to a race condition under heavy load with multiple MAC addresses being presented to dot1x and Auth Manager framework at the same time. This problem is not present with default (single) hostmode.
  The issue can only occur if multiple authentication methods are configured on the port, so just dot1x configured on a port will not trigger the problem, it has to be, for example, dot1x and MAB.
  The issue cannot occur if dot1x is not configured on a port( e.g.: for just MAB).
  Workaround: Issue `dot1x re-authenticate interface` on the affected ports.

• CSCtq29554
  Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the `show ipc port | in MRIB` command on a failed line card does not display a port.
  Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover.  The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.
  Workaround: Reload the failing line card to recover it.

• CSCtq31898
  Symptoms: Web traffic is not getting redirected to scansafe towers.
  Conditions: Having dual WAN links to reach the scansafe tower and the source interface used as a loopback.
  Workaround: There is no workaround.

• CSCtq33932
  Symptoms: Unable to configure a command under the ATM subinterface.
  Conditions: The symptom is observed when you delete an ATM subinterface and re-create the same. Unable to configure commands under this ATM subinterface.
  Workaround: Create an ATM subinterface with a ID different to that of the one deleted earlier.
• CSCtq36153
   Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:
   - Memory Leak Associated with Crafted IP Packets
   - Memory Leak in HTTP Inspection
   - Memory Leak in H.323 Inspection
   - Memory Leak in SIP Inspection
   Workarounds that mitigate these vulnerabilities are not available.
   Cisco has released free software updates that address these vulnerabilities.
   This advisory is available at the following link:
   http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

• CSCtq36192
   Symptoms: Cisco IOS with Zone Based Firewall crashes the router.
   Conditions: The issue is seen when modifying the parameter map as shown below:
   parameter-map type regex slim no pattern [^x80]
   Workaround: There is no workaround.

• CSCtq37579
   Symptoms: Enabling and disabling “snmp-server traps” crash the UUT.
   Conditions: The symptom is observed when you disable the snmp-server and do a write memory.
   Workaround: There is no workaround.

• CSCtq39406
   Symptoms: When you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM, the module shuts down after 2 minutes. Then, all IP connectivity and console connectivity to the router is lost.
   Conditions: This symptom occurs when you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM.
   Workaround: Remove the HWIC-3G-HSPA. When you remove the 3G module from the system, energywise works as expected. You can shut down power modules using the above configuration. As soon as the 3G card is installed in slot 2 or 3 and the energywise level is set to zero, the service module shuts down and the entire router crashes. It has no IP connectivity and the console is inactive. The only workaround is a hard reset (along with removal of the card).

• CSCtq45553
   Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:
   - Memory Leak Associated with Crafted IP Packets
   - Memory Leak in HTTP Inspection
   - Memory Leak in H.323 Inspection
   - Memory Leak in SIP Inspection
   Workarounds that mitigate these vulnerabilities are not available.
   Cisco has released free software updates that address these vulnerabilities.
This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

- **CSCtq47856**
  Symptoms: The following issues are observed:
  1. Crypto map is configured with a local ACL at registration time.
  2. Local ACL is removed from global configuration (without removing it from the crypto map configuration).
  3. Remove crypto map from the interface.
  Issue 1: At this point `show crypto gdoi` continues to display the TEK SA, even though the GM has no interfaces configured with a crypto map.
  4. Re-apply the crypto map to the interface and let registration complete.
  Issue 2: If `crypto gdoi ks rekey` is issued on the keyserver, then `show crypto gdoi` continues to display only the old TEK. New TEKs installed by subsequent rekeys are not displayed.
  5. On the keyserver, issue `crypto gdoi ks rekey replace`.
  Issue 3: GM crashes in the IPSec code while processing the new SAs and shortening the old ones.
  Conditions: The symptom is observed on a router that is running GET VPN.
  Workaround: Remove the ACL from the crypto map configuration before removing it from the global configuration.

- **CSCtq49325**
  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.
  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.
  Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.
  Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- **CSCtq49860**
  Symptoms: If an ISM VPN module is installed in the Cisco ISR G2 platform, export limits will be exceeded without an HSECk9 license installed.
Caveats for Cisco IOS Release 15.2(2)T

Conditions: The symptom is observed with an ISM VPN module installed and enabled for crypto acceleration.
Workaround: There is no workaround.

- CSCtq52655
  Symptoms: Unable to route packets through the router, specifically when testing ICMP traffic.
  Conditions: This happens when using the VMI in aggregate mode. It only appears to occur with IPv6.
  Workaround: Turn off IPv6 CEF.

- CSCtq55173
  Symptoms: A device that is configured with NAT crashes. SIP appears to be translated through NAT. However, some cases report that the crash still occurs after redirecting SIP traffic elsewhere.
  Conditions: The crash is triggered when the clear ip nat translation *, clear ip nat translation forced, or clear crypto ipsec client ezvpn command is entered.
  Workaround: There is no workaround.

- CSCtq56948
  Symptoms: The default route attribute is used by features like uRPF and if it is missed out, it may cause uRPF to allow packets whose source addresses match against the default route.
  Conditions: This symptom occurs because some prefixes in the FIB are sourced by non-RIB features, such as CTS, or are used to represent next hops for recursive paths. Such prefixes inherit the forwarding information from their covers, but the default route attribute is not inherited.
  Workaround: There is no workaround.

- CSCtq58383
  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.
  Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.
  Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq60703
  Symptoms: The device crashes and traceback is seen when executing write network.
  Conditions: The symptom is observed when the command write network is used with no URL specified.
  Workaround: Specify a URL.

- CSCtq62322
  Symptoms: On an SNR call, when the call is forward and connected to CUE after ringing to the remote target, nothing happens (for example, no CUE prompt occurs, and the user cannot leave voice mail).
  Conditions: This symptom is observed if the answer-too-soon timer is configured, the remote target is a pstn call, and the calling party is using a sccp phone.
  Workaround: There is no workaround.
• CSCtq62759
  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.
  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.
  Workaround: Use the clear clns route command or the clear isis * command.

• CSCtq63225
  Symptoms: Packet drop seen when running traffic.
  Conditions: The symptom is observed when IPSec along with QoS is configured.
  Workaround: There is no workaround.

• CSCtq63838
  Symptoms: A Cisco 2921 router crashes, and the following traceback is seen:

  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback= 0x24A19810z 0x24A5DC8Cz 0x24A4A560z 0x24DF6618z 0x24DF6BBcz 0x24A2DD5Cz 0x24A2E274z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback= 0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBcz 0x24A2DD5Cz 0x24A2E274z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z 0x24DF6BBcz 0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
  %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 315556E0. -Process= "DSMP", ipl= 0, pid= 306, -Traceback= 0x246EBB2Cz 0x24719984z 0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBcz 0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z

  Conditions: This symptom is observed with the DSMP process.
  Workaround: There is no workaround.

• CSCtq64034
  Symptoms: NAT does not send gratuitous ARP for a translated address when an interface comes up.
  Conditions: The symptom is observed when an alias (translated address) is created with the interface (whose IP address is in the same subnet as the alias entry) is in shut down state.
  Workaround: Perform an admin shut/no shut on the interface with an IP address in the same subnet as the alias entry.

• CSCtq67750
  Symptoms: In relation to caveat CSCtn52350, before-after is on without it having been turned on.
  Conditions: The symptom is observed when the following CLI is configured:

  archive
  log config
  logging persistency

  Workaround: Remove “logging persistency” from the configuration:

  archive
  log config
  no logging persistency

• CSCtq68778
  Symptoms: After an ISSU, the reload reason string is missing in the newly-active session.
  Conditions: The symptom is observed after an ISSU.
  Workaround: There is no workaround.
• CSCtq71011
Symptoms: The router crashes, or in some cases a traceback is seen.
Conditions: This symptom is seen when IPv6 routes with diverse paths are enabled.
Workaround: There is no workaround.

• CSCtq71344
Symptoms: Sometimes HTTPS sessions may fail when they are redirected via a Scansafe tower.
Conditions: This symptom is observed when multiple HTTPS sessions are being redirected to Scansafe towers by the content-scan feature.
Workaround: White-list the HTTPS traffic not to be redirected to SS towers by applying an ACL in the content-scan configuration.

• CSCtq72873
Symptoms: A crash is caused when a MAB client fails to authenticate and is simultaneously deleted from the switch. This caveat has only been seen on the Cisco Catalyst 6k switch, but it potentially also affects the Cisco Catalyst 3k and 4k families.
Conditions: The switch port must be configured for MAB. A MAB client must connect and then simultaneously it must be deleted and fail authentication. This is a race condition and so this bug is rarely seen.
The failure of authentication could be caused by the ACS server rejecting the MAB request or the ACS server being unavailable. The deletion of the MAB client on the switch can be caused by shutting down the MAB enabled interface or issuing the clear authentication sessions CLI.
Workaround: There is no workaround for this issue other than disabling MAB on the interface. However for the crash to happen the MAB client must be deleted from the switch. Avoiding shutting down the MAB-enabled interface and avoiding any CLI that clears the MAB session, will reduce the risk of the switch crashing.

• CSCtq75008
Symptoms: A Cisco 7206 VXR crashes due to memory corruption.
Conditions:
- The Cisco 7206 VXR works as a server for L2TP over IPsec.
- Encryption is done using C7200-VSA.
- More than two clients are connected.
If client sessions are kept up for about a day, the router crashes.
Workaround: There is no workaround.

• CSCtq75045
Symptoms: When a router is running FlexVPN-IKEv2 in auto-reconnect mode, IPSec SAs are not renegotiated properly after a clear crypto session command is entered. Entering the show crypto ikev2 client flexvpn command will indicate that the router is in a NEGOTIATING state.
Conditions: This symptom is observed on a router running FlexVPN on IKEv2 in auto-reconnect mode.
Workaround: Enter the clear crypto ikev2 client flexvpn command to clear the FlexVPN state and renegotiate the SAs successfully.
Caveats for Cisco IOS Release 15.2(2)T

- **CSCtq76005**
  Symptoms: Configuring “atm route-bridge ip” on an MPLS-enabled ATM interface makes router punt all incoming MPLS packets to CPU.
  Conditions: The symptom is observed when RBE is configured on an MPLS-enabled ATM interface.
  Workaround: Remove RBE.

- **CSCtq77024**
  Symptoms: Metrics collection fails on hop0 if route change event occurs.
  Conditions: This symptom is observed when the mediatrace is not passing up an interface type that is acceptable to DVMC when a route change occurs on the node which has the initiator and responder enabled.
  Workaround 1: Remove and reschedule mediatrace session.
  Workaround 2: Remove and reconfigure mediatrace responder.

- **CSCtq77274**
  Symptoms: FXS phones are not recognized as SCCP endpoints.
  Conditions: This symptom occurs when FXS phones are configured as SCCP endpoints.
  Workaround: There is no workaround.

- **CSCtq77363**
  Symptoms: License images are not working properly.
  Conditions: This symptom is seen when the license image is loaded. There is a traceback due to access of uninitialized variables.
  Workaround: There are no workarounds.

- **CSCtq78217**
  Symptoms: A router crashes with the following information:
  System returned to ROM by address error at PC 0xZZZZZZZZ, address 0xZZZZZZZZ
  Conditions: The symptom is observed with CUBE + SIP.
  Workaround: There is no workaround.

- **CSCtq79382**
  Symptoms: In the HA setup and on the Active, if you have a probe configured with VRF and you remove the VRF with `no ip vrf vrflname` and reboot, it keeps rebooting again and again (crashes).
  Conditions: The symptom is observed when removing the VRF and rebooting the Active terminal.
  Workaround: Check that the system is in standby and that there is no VRF configured. Even though there is a probe configured with VRF, you can proceed without crashing the Active after a reboot.

- **CSCtq80477**
  Symptoms: Invalid input detector with “no interface serial multipoint” interface.
  Conditions: CSCto98742 fix was causing the chain breakage in the “no” form of the CLI.
  Workaround: There is no workaround.

- **CSCtq80648**
  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.
For example:

```plaintext
interface Ethernet1/0
  vrf forwarding vpn1
  ipv6 address 1::1/64
!
router bgp 65000
  address-family ipv6 vrf vpn1
  neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
```

If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

Conditions: This symptom occurs when a user changes the VRF assignment.

Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq83257
  Symptoms: A Cisco 870 platform router crashes while booting with an advipservices image.
  Conditions: This symptom is observed on a Cisco 870 platform router running Cisco IOS Release 15.2(0.18)T and while booting with an advipservices image.
  Workaround: There is no workaround.

- CSCtq83468
  Symptoms: 302 Page Moved to url: https://<virtual-ip>/login.html?redirect-url=<actual-url> does not happen, and the client is directly presented with the login page.
  Conditions: The Proxy Auth method and ip admission virtual-ip should be configured.
  Workaround: Unconfigure ip admission virtual-ip.

- CSCtq84635
  Symptoms: Trunk DNs can act as if busy (such as by triggering CFB) even though they have no calls and show commands for ephone-dns or ports report nothing unusual.
  Conditions: This symptom occurs in Cisco IOS Release 15.0(1)M after heavy use; it is believed not to occur in Cisco IOS Release 12.4(20)T or prior releases.
  Workaround: Delete and re-add trunk DNs.

- CSCtq85564
  Symptoms: The fix of CSCto77352 may cause a data corruption problem.
  Conditions: This symptom is seen when two processes are calling the same function that is raising the race condition.
  Workaround: There is no workaround.

- CSCtq85728
  Symptoms: An EHWIC-D-8ESG card is causing an STP loop.
  Conditions: EHWIC-D-8ESG might not be blocking appropriate ports according to calculated STP topology that introduces the loop in the network.
  Workaround: There is no workaround.
- **CSCtq86500**
  Symptoms: With the fix for CSCtf32100, clear text packets destined for the router and coming into a crypto-protected interface are not switched when VSA is used as the crypto engine.
  Conditions: This symptom occurs with packets destined for the router and coming in on an interface with the crypto map applied and VSA as the crypto engine.
  Workaround: Disable VSA and use software encryption.

- **CSCtq86515**
  Symptoms: UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.
  Conditions: This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.
  Workaround: Do not drop traffic on the device sending the UDP Jitter probe.

- **CSCtq88777**
  Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.
  Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.
  Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- **CSCtq90054**
  Symptoms: `nbar protocol-discovery` fails to recognize Skype application traffic.
  Conditions: The issue is seen after configuring PfR to control NBAR based application traffic.
  Workaround: There is no workaround.

- **CSCtq90577**
  Symptoms: A router crashes when removing Netflow.
  Conditions: The symptom is observed when removing Netflow.
  Workaround: There is no workaround.

- **CSCtq91176**
  Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and LNS does renegotiation, then the PPP session cannot be established.
  Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.
  Workaround 1: Disable lcp renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.
  Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- **CSCtq91305**
  Symptoms: Standby cannot reach HOT sync state with active. The standby RP keeps resetting. The following message is displayed:
  *Apr 18 15:38:47.704: %SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1), process = IPC Dynamic Cache.*
  Conditions: This symptom occurs with SSO mode, when the Cisco ASR1k is configured with ISG as dhcp server and with a low dhcp lease timer.
  Workaround: There is no workaround.
• CSCtq91939
  Symptoms: Intermittent crash due to SegV Exception after a consult transfer of external SIP call to a local ephone extension.
  Conditions: The symptom is observed under the following conditions:
  – UC540 that is running Cisco IOS Release 15.1(2)T3.
  – CME 8.1.
  – SIP----UC540---switch--SCCP---IP phones.
  Workaround: There is no workaround.

• CSCtq92182
  Symptoms: An eBGP session is not established.
  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.
  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

• CSCtq92650
  Symptoms: DMVPN tunnel is not selecting the right source interface.
  Conditions: The symptom is observed when multi-link frame relay creates more than one subinterface with the same name.
  Workaround: There is no workaround.

• CSCtq92940
  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.
  Conditions: This symptom may be seen when an active FTP connection is used (that is, the no ip ftp passive command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.
  Workaround: Use passive FTP (default) by configuring the ip ftp passive command.
  Further Problem Description: Please see the original bug (CSCtl19967) for more information.

• CSCtq95566
  Symptoms: CUCM will append “:5060” to the contents of a contact header when building an outgoing URI if no other port is specified. This is incorrect per the RFC3261. For example: If the following header is received in the contact header of a 200 OK:

  Contact: <sip:555112222@192.168.1.1;gr=urn:uuid:44022016-d652-53cf-96e2-8421b7e3dbf5>

  CUCM will build the URI of the ACK as:

  ACK sip:555112222@192.168.1.1:5060;gr=urn:uuid:44022016-d652-53cf-96e2-8421b7e3dbf5 SIP/2.0

  Conditions: This was is on a Cisco Unified Communications Manager Release 8.6 (1).
  Workaround: There is no workaround.

• CSCtq96329
  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.
  Conditions: This symptom can happen only when bgp deterministic-med is configured.
The following releases are impacted:
- Cisco IOS Release 15.0(1)S4
- Cisco IOS Release 15.1(2)T4
- Cisco IOS Release 15.1(3)S
- Cisco IOS Release 15.2(1)T

Workaround: Disable deterministic med in the network/AS by issuing the `no bgp deterministic-med` command and then the `clear ip bgp *` command or hardreset of BGP session to remove any stale prefixes.

It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- **CSCtq96466**
  Symptoms: The interface configuration “ipv6 dhcp client pd <pd-name>” is not shown in the running-config under virtual-template interfaces.
  Conditions: This happens when the above CLI is configured on a virtual-template interface.
  Workaround: There is no workaround.

- **CSCtq96544**
  Symptoms: Application ID is limited to 100.
  Conditions: The symptom is observed when configuring a new application. The application ID only allows values in the range of 0-100.
  Workaround: There is no workaround.

- **CSCtq97883**
  Symptoms: Traceback is shown. The root cause is a null pointer.
  Conditions: The symptom is observed during longevity testing of Cisco IOS Release 12.4(24)GC3a and Cisco IOS Software 15.1(2)GC.
  Workaround: There is no workaround.

- **CSCtr01750**
  Symptoms: The command `clear ip nat translation *` is not working as expected.
  Conditions: Issue is seen with a Cisco 7200 platform that is running the Cisco 15.2 (0.19)T0.1 image. This issue is specific to the NAT translations created for ICMP traffic sent with port number 0.
  Workaround: There is no workaround.

- **CSCtr01957**
  Symptoms: System crashes when doing a `crypto engine slot 0`.
  Conditions: The symptom is observed with a system boot up with no `crypto engine slot 0`.
  Workaround: There is no workaround.

- **CSCtr04829**
  Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.
Caveats for Cisco IOS Release 15.2(2)T

Caveats

Conditions: This symptom occurs when the hardware address is zero.
Workaround: There is no workaround.

- CSCtr06926
Symptoms: A CA server in auto grant mode goes into disabled state when it receives a client certificate enrolment request.
Conditions: The symptom is observed when a client certificate enrolment request is received.
Workaround: Do not place the CA server in auto grant mode.

- CSCtr07142
Symptoms: A memory leak is seen at crypto_ss_open.
Conditions: No special configuration is needed.
Workaround: There is no workaround.
Further Problem Description: At bootup, when the `show memory debug leaks` command is run, memory leak entries are seen for the crypto_ss_open process.

- CSCtr09142
Symptoms: Poor throughput is observed with content-scan.
Conditions: This symptom occurs when content-scan is enabled.
Workaround: There is no workaround.

- CSCtr09251
Symptoms: Continuous alignment errors and performance degradation in throughput of MS RPC traffic through the ZBFW.
Conditions: The symptom is observed when inspecting MS RPC traffic through the ZBFW on a Cisco 2911 router that is running Cisco IOS Release 15.1(4)M.
Workaround: There is no workaround.

- CSCtr10577
Symptoms: The following error message may be seen:
`OCE-3-OCE_FWD_STATE_HANDLE limit reached`.
Conditions: This symptom is observed under high traffic.
Workaround: There is no workaround.

- CSCtr11620
Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.
Conditions: This symptom is observed when a Cisco 2911 is used.
Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr13172
Symptoms: The `config replace` command crashes the router.
Conditions: The symptom is observed when close to the maximum number of mediatrace and performance monitoring policies along with DMVPN are configured on the router and the target configuration contains none of these elements.
Workaround: Uninstall the mediatrace and performance monitor policies prior to replacing the configuration.
• CSCtr14763
Symptoms: A BFD session is always up, although the link protocol is down.
Conditions: First the BFD session is up between the routers. After the VLAN is changed on the switch between the routers, the BFD peer is not reachable but the BFD sessions are always up.
Workaround: There is no workaround.

• CSCtr18559
Symptoms: An unallocated/unassigned number is received from PBX but as a response, a network congestion message is sent back. Gateway rejects call with 4# when actually its supposed to send a 7#.
Conditions: The issue occurs only when the country Brazil is configured. When country is set to “itu”, then a 5# is sent which is correct for an unallocated/unassigned number. Follow this link to track cause code to CAs mapping based on selection of countries:
http://www.pulsewan.com/data101/r2mfc.pd
Workaround: There is no workaround.

• CSCtr18574
Symptoms: H323-H323 video calls fail with cause code 47.
Conditions: The symptom is observed when an H323-H323 video call fails to establish an H245 media connection. The following errors are seen:
Received event H225_EV_H245_FAILED while at state H225_WAIT_FOR_H245
cch323_send_passthru_out: Send passthru message retcode 15
Workaround: There is no workaround.

• CSCtr19922
Symptoms: Lots of output printed by show adjacency [key of adj] internal dependents followed by a crash.
Conditions: The symptom is observed with the existence of midchain adjacencies, which will be created by IP tunnels, MPLS TE tunnels, LISP, and similar tunneling technologies.
Workaround: Do not use the show adjacency [key of adj] internal dependents command. Specifically, it is the “dependents” keyword which is the problem. If the dependents keyword is not used there is no problem.

• CSCtr20300
Symptoms: SA negotiation test is failing for ipsec_core script.
Conditions: The symptom is observed when the SA should come into idle state after using show crypto isakmp sa.
Workaround: There is no workaround.

• CSCtr20908
Symptoms: A spurious access will occur on platforms that detect spurious accesses. A crash will occur on platforms that do not detect spurious accesses such as the Cisco ASR 1000, Cisco 3900 and 3900e.
Conditions: The issue occurs when running the show run all command and when WEBVPN configurations are present.
Workaround: Use the Cisco IOS 15.1(3)T train.
- **CSCtr23134**
  Symptoms: Crash seen when IKEv2 debugs are enabled.
  Conditions: The symptom is observed when using the debug “debug crypto ikev2 internal.”
  Workaround: There is no workaround.

- **CSCtr25734**
  Symptoms: A router crashes.
  Conditions: This symptom is observed when the router is reloaded with a BRI interface brought up in startup configuration.
  Workaround: There is no workaround.

- **CSCtr25821**
  Symptoms: A Cisco 800 series router crashes with `isdn leased-line bri0 128` command:
  ```
  Unexpected exception to CPU: vector 1000, PC = 0x0 , LR = 0x8155A310
  ```
  Conditions: The symptom is observed with the `isdn leased-line bri0 128` command.
  Workaround: The issue does not occur if there is no cable that connects to the BRI interface. Disconnect the cable from the BRI interface while `isdn leased-line bri0 128` is configured.

- **CSCtr26531**
  Symptoms: When you disable the ISM VPN accelerator using `no crypto engine slot 0`, the ISM VPN module is not disabled.
  Also, under a high load the ISM VPN firmware download will fail.
  Conditions: The symptom is observed with an ISM VPN module and during high traffic load.
  Workaround: There is no workaround.

- **CSCtr28857**
  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.
  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

- **CSCtr29338**
  Symptoms: A router crashes.
  Conditions: The symptom is observed after an `%ISDN-6-DISCONNECT` message from “unknown” followed by a couple of “Illegal Access to Low Address” messages.
  Workaround: There is no workaround.

- **CSCtr31153**
  Symptoms: Packet decryption seems to fail with manual crypto maps configured on interface.
  Conditions: The symptom is observed on a Cisco 7200 series router loaded with Cisco IOS interim Release 15.2(0.19)T0.1.
  Workaround: There is no workaround.
• CSCtr33856
  Symptoms: Traceback and/or watchdog crash, with decodes pointing to mace_monitor_waas_command@

  %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 218959117 for chunk 6527D73C, data D0D0D0D -Process= "Exec", ipl= 0, pid= 373 -Traceback= 23054C68z 2238121Cz 223877F0z 22397A24z 2376B0FCz 2376B0E0z or %SYS-2-FREEBAD: Attempted to free memory at 4F, not part of buffer pool -Traceback= 24F4EA90z 23789608z 237758E4z 23054C68z 2238121Cz 223877F0z 22397A24z 2376B0FCz 2376B0E0z %SYS-2-NOTQ: unqueue didn’t find 4F in queue 28275D8C -Process= "Exec", ipl= 4, pid= 374

  Conditions: The symptom is observed with on the fly changes to mace policies and classes.

  Workarounds: There is no workaround.

• CSCtr34965
  Symptoms: An SSL WebVPN page does not come up when ISM-VPN is used.

  Conditions: When an attempt is made to bring up an SSL session with ISM-VPN, the page does not load.

  Workarounds: There is no workaround.

• CSCtr35740
  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.

  Conditions: The symptom is observed when the DMVPN tunnel active link goes down.

  Workarounds: There is no workaround.

• CSCtr38563
  Symptoms: Switch crashes after configuring a secondary IP address. If the address is saved previously and the switch is upgraded, it will enter a crashing loop.

  Conditions: This occurs when configuring a secondary IP address on a VLAN interface.

  Workarounds: There is no workaround.

• CSCtr40091
  Symptoms: A call is not recorded.

  Conditions: This symptom is observed after a few days of load.

  Workarounds: There is no workaround.

• CSCtr42341
  Symptoms: Crash at task_execute_prep.

  Conditions: The symptom is observed with a Cisco 800 series router that is configured with BFD.

  Workarounds: There is no workaround.

• CSCtr42913
  Symptoms: Stale crypto maps seen even after unconfiguring tunnel protection.

  Conditions: The symptom is observed when removing the tunnel source configuration.

  Workarounds: Unconfigure and configure again or unconfigure tunnel protection first.

• CSCtr44686
  Symptoms: There is a crash after matching traffic and resetting the connection using following maps:

  policy-map type inspect smtp SMTP_L7_P1
Caveats

```plaintext
class type inspect smtp SMTP_L7_C1 reset
policy-map type inspect smtp SMTP_L7_P2
class type inspect smtp SMTP_L7_C2A reset
class type inspect smtp SMTP_L7_C2B reset
```

Conditions: The symptom is observed with the above maps.

Workaround: Replace “reset” with “log”.

- **CSCtr44864**
  
  Symptoms: SYS-2-MALLOCFAIL error message with a device configured with ZBFW and Layer FTP application inspection.

  Conditions: Will observe the following console log messages: %SYS-2-MALLOCFAIL: Memory allocation of 214 bytes failed from 0x22349EA4, alignment 0 Pool: Processor Free: 604021800 Cause: Interrupt level allocation Alternate Pool: None Free: 0 Cause: Interrupt level allocation Process= "<interrupt level>", ipl= 1

  Workaround: Disable FTP Application Inspection.

- **CSCtr45608**
  
  Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

  Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.

  Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

- **CSCtr45633**
  
  Symptoms: A BGP dynamic neighbor configured under VPNv4 address-family does not work correctly.

  Conditions: The symptom is observed when a BGP dynamic neighbor is configured under a VPNv4 address-family.

  Workaround: Add “dynamic neighbor peer-group” under “ipv4 unicast address- family”.

- **CSCtr45978**
  
  Symptoms: Cisco IOS WAAS has FTP connections hung in CONN_ABORT state.

  Conditions: Device configured with Cisco IOS WAAS, and crafted FTP packets are passed across the WAN link. Has only been observed on 15.2(1)T IOS Code.

  Once the connection limit is reached and the rest of the connections started going pass-through.

  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.1:


No CVE ID has been assigned to this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:

Caveats for Cisco IOS Release 15.2(2)T

CSCtr49064
The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

CSCtr50118
Symptoms: The router crashes.
Conditions: This symptom occurs when the presence feature is turned on.
Workaround: There is no workaround.

CSCtr51786
Symptoms: The command passive-interface for a VNET auto-created subinterface x/y.z may remove the derived interface configuration command ip ospf process id area number. Consequently, putting back no passive-interface command will not form the lost OSPF ADJ.
Conditions: The symptom is observed only with interfaces associated with the OSPF process using the command ip ospf vnet area number.
Workaround: Associate the interface with the OSPF process using a network statement or using the interface command ip ospf process id area number.

Further Problem Description: Interfaces associated with a process using a network statement under “router ospf” or interfaces configured with the command ip ospf process id area number are not affected.

CSCtr51926
Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.
Conditions: The symptom is observed when a service-policy is applied on the main interface.
Workaround 1: Enable IPv6 explicitly on the main interface:
interface x/y ipv6 enable
Workaround 2: Reconfigure the IPv6 address on the subinterface:
interface x/y.z no ipv6 address ipv6 address ...

CSCtr52186
Symptoms: Console will not time out from exec session.
Conditions: The symptom is observed when the router is booted up with “exec-timeout 0 0” for the particular TTY.
Workaround: Configure significant exec-timeout value and “exit” from exec mode.
Caveats

- **CSCtr52740**
  Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.
  Conditions: The symptom is observed when querying history information from rttMonHistoryCollectionCompletionTime object using invalid indices.
  Workaround: Instead of using “get”, use “getnext” to list valid indices for the MIB OID.

- **CSCtr53944**
  Symptoms: IPv6 unicast packets are dropped.
  Conditions: The symptom is observed when there is a breakage in VMI fastpath when passing IPv6 unicast packets.
  Workaround: There is no workaround.

- **CSCtr54269**
  Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.
  Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.
  Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

- **CSCtr54327**
  Symptoms: A Cisco router may crash due to a SegV exception or have a spurious access when a fax comes in.
  Conditions: The crash occurs on a voice gateway that is configured with transcoding and fax passthrough where a fax call comes in for a codec, but the fax is not configured for a codec, and the “a=silenceSupp:off” option is set in SDP.
  Workaround: There is no workaround.

- **CSCtr54907**
  Symptoms: A router crashes.
  Conditions: This symptom is observed when an ISM VPN accelerator is used as the crypto engine.
  Workaround: Disable the ISM VPN accelerator.

- **CSCtr55348**
  Symptoms: Seemingly unending MIB walk.
  Conditions: The symptom is observed when auto-generated IP SLA probes are present and a MIB walk encompassing either rttMonReactTriggerAdminStatus or rttMonReactTriggerOperTable is done.
  Workaround: There is no workaround.

- **CSCtr57804**
  Symptoms: ASR 1K router may delete “ipv6 prefix no-advertise” configuration from its subinterfaces when the subinterface is shut down. This may also be seen after a router reload.
  Conditions: This issue is seen when the prefixes defined on the subinterface have been inherited from the “ipv6 general-prefixes" defined in the configuration.
  Workaround: Remove “ipv6 general-prefixes” from the configuration.

- **CSCtr58140**
  Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.
Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

Workaround: There is no workaround.

- CSCtr59314
  Symptoms: A router reloads when the clear crypto session command is issued with 4000 sessions up.
  Conditions: This symptom is observed only under load conditions.
  Workaround: There is no workaround.

- CSCtr59775
  Symptoms: Proxy map-reply reports locator as unreachable/down.
  Conditions: The symptom is observed when ETR registers to a map-server with proxy map-reply turned on.
  Workaround: Turn-off proxy map-replying.

- CSCtr59840
  Symptoms: Crypto tunnels may flap up and down constantly after issuing a clear crypto session or clear crypto isakmp and clear crypto sa.

RTR#clear cry sess
RTR#
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer 10.10.1.1:500
Id: serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN,
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer 10.10.10.10:500
Id: serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN,
RTR#
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP . Peer 10.10.1.1:500
Id: serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN,
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP . Peer 10.10.10.10:500
Id: serialNumber=xxxxxx+hostname=RTR,c=US,o=TEST,ou=TEST VPN,
...

Conditions: This issue is seen when using eToken and OCSP revocation check on Cisco 870, 881, 1812 and 1921 routers that are running Cisco IOS Release 15.1 (2)T3. Certificate-based authentication is also used.

Workaround: Disabling OCSP revocation check, if configured, may alleviate this behavior.

- CSCtr61289
  Symptoms: FlexVPN client remains in NEGOTIATING state, despite being on auto-connect mode, when the FlexVPN server executes a clear crypto session.
  Conditions: This occurs in a dVTI setting, where the server has a virtual-template interface and the client has a static tunnel interface that connects to the server. This is not observed in a static setting.
  Workaround: On the client, issue a clear crypto ikev2 client flexvpn to clear the FlexVPN session and allow the client to reconnect to the server again.

- CSCtr63462
  Symptoms: A router crashes at bootup.
  Conditions: This symptom is observed with a Cisco 3900 that has an ISM VPN module installed and no HSECk9 license installed.
  Workaround: Boot with a pre-15.2(1)T image, load an HSECk9 license, and then boot with a 15.2(1)T image.
Caveats

- **CSCtr66487**
  Symptoms: Packet drops beyond 1492 MTU size with MPLS L2VPN Xconnect configuration.
  Conditions: The symptom is observed when you ping mpls pseudowire 10.0.0.1 101 size 1493 and above.
  Workaround: There is no workaround.

- **CSCtr66630**
  Symptoms: There is prefix corruption when configuring 6VPE. Advertised prefix is different than the one installed. RD value also changes as well.
  Conditions: The symptom is observed when configuring “vpnv6 address family”.
  Workaround: There is no workaround.

- **CSCtr71465**
  Symptoms: A router crashes at ipv4fib_les_switch_fastswitching_compat while booting.
  Conditions: The symptom is observed on a Cisco 888E router that is running Cisco IOS interim Release 15.1(2)T1.1 or later.
  Workaround: There is no workaround.

- **CSCtr75399**
  Symptoms: Incremental chunk leaks at NBAR FO chunk and NBAR Flowvar chunk.
  Conditions: The issue is seen in a steady state scenario.
  Workaround: There is no workaround.

- **CSCtr83533**
  Symptoms: When you check the message on a VM system and that triggers the SIP notify to turn off the MWI to IAD, IAD will turn off the MWI but, after that, DSP is not released for the port. If you make one more call, in the next call you will hear silence. After it is off hook, there is no ring tone.
  Conditions: The symptom is observed when MWI is configured for analog ports on IAD, and if MWI is ON and a call is made to clear the MWI.
  Workaround 1: Reload the router.
  Workaround 2: Remove the MWI configuration from the analog port configuration.

- **CSCtr83542**
  Symptoms: When content-scan functionality is enabled, the throughput drastically comes down and CPU utilization approaches 100 percent.
  Conditions: This symptom is observed when content-scan is enabled and web traffic is subjected to redirection.
  Workaround: Disable content-scan functionality.

- **CSCtr84800**
  Symptoms: An accounting stop is not triggered from DHCP when a client releases the binding.
  Conditions: A DHCP server has a pool with accounting set. When a DHCP client releases the lease, an accounting stop is not sent.
  Workaround: There is now workaround.
• CSCtr86077
  Symptoms: MGCP call drops 10 seconds after IP phone puts call on hold.
  Conditions: The symptom is observed under the following conditions:
  – IP phone -- CUCM -- MGCP -- GW -- PRI.
  – “mgcp rtp unreachable timeout 10000” is configured on gateway.
  – “no MOH” is configured for the IP phone so Tone on Hold (TOH) is used.
  – IP phone make calls to PSTN and is answered.
  – IP phone puts call on hold.
  – PSTN user hears TOH.
  – 10 seconds after hold is initiated, call is dropped.
  Workaround: Remove “mgcp rtp unreachable timeout” from the MGCP gateway.

• CSCtr86437
  Symptoms: NAT-PT function does not work properly after an interface flap occurs.
  Conditions: The symptom is observed when you configure NAT-PT on the router.
  Workaround: Reconfigure “ipv6 nat prefix.”

• CSCtr87249
  Symptoms: A Cisco 2900 router crashes while it is reloaded with a 15.2(1.6)T image.
  Conditions: This symptom occurs when an ISM-VPN card is installed on the Cisco 2900 and when there is no HSECK9 license installed.
  Workaround: When the HSECK9 license is installed on the Cisco 2900, the crash is not seen.

• CSCtr87740
  Symptoms: A router may crash due to a bus error.
  Conditions: The symptom seems to be related to high traffic and an ongoing rekey taking place.
  Workaround: There is no workaround.

• CSCtr89322
  Symptoms: NME-RVPN module is not recognized by a Cisco 3900e router.
  Conditions: The symptom is observed with a Cisco 3900e router.
  Workaround: There is no workaround.

• CSCtr89882
  Symptoms: Platform-related error messages are seen during an LDP flap in an ECM scenario.
  Conditions: This symptom is observed with LDP with ECMP paths and during flapping of LDP sessions.
  Workaround: There is no workaround.

• CSCtr91106
  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.
  Products that are not running Cisco IOS Software are not vulnerable.
Cisco has released free software updates that address these vulnerabilities. The HTTP server may be disabled as a workaround for the vulnerability described in this advisory. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- **CSCTR91890**
  
  **Symptoms:** An RP crashes sometimes when the router is having PPPoX sessions.
  
  **Conditions:** If a PPPoX session is terminated in the middle of session establishment and ip local pool is configured to pick the IP address for the peer and the version that the router is running has the fix for CSCTR91890.
  
  **Workaround:** There is no known workaround.

- **CSCTR94052**
  
  **Symptoms:** Tracebacks seen for Call Forward to CUE scenarios.
  
  **Conditions:** The issue is observed from Cisco IOS interim Release 15.2(1.3)T and onwards.
  
  **Workaround:** There is no workaround.

- **CSCTR94887**
  
  **Symptoms:** Using MRCP v1, VXML script with ASR operation will always receive noinput event.
  
  **Conditions:** The symptom is observed with Cisco IOS Release 15.2(1)T.
  
  **Workaround:** There is no workaround.

- **CSCTR97248**
  
  **Symptoms:** Router reloads with the following:

  Unexpected exception to CPU: vector 300, PC = 0xZZZZZZZZZ, LR = 0xXXXXXXXX
  
  **Conditions:** The symptom is observed with L4F (TCP Proxy) based NAT ALG processing of TCP DNS traffic.
  
  **Workaround:** Use the following configuration:

  ```
  Router(config)# no ip nat service tcp-alg
  ```

- **CSCTS01653**
  
  **Symptoms:** Spurious memory access seen on video monitoring router.
  
  **Conditions:** The issue is seen after recreating the interface.
  
  **Workaround:** There is no workaround.

- **CSCTS04963**
  
  **Symptoms:** The following spurious access is seen:

  No alignment data has been recorded.
  
  Total Spurious Accesses 789, Recorded 1
  
  Address Count Traceback 0 789 0x23342B70z 0x239B3450z
  
  Decodes:

  ```
  0x23342B70:csdb_dp_timer_handle_flow_idle_timeout(0x233429ac)+0x1c4
  0x239B3450:tw_notify(0x239b3394)+0xbc
  ```
  
  **Conditions:** The symptom is observed when MACE and WAAS are configured on the router. While running traffic, spurious memory access is seen. The number of spurious memory accesses indicate that this is continuously happening while timer events are triggered. This is usually seen within 10 minutes of running traffic. After a random amount of time, the router hangs and there is no response. A send break has to be sent at the console to recover to rommon.
Caveats for Cisco IOS Release 15.2(2)T

Caveats

Workaround: There is no workaround.

- CSCts06776
  Symptoms: Requests hang when NAT is enabled.
  Conditions: This symptom is observed when content scan and NAT are enabled.
  Workaround: There is no workaround.

- CSCts11594
  Symptoms: A mediatrace session is scheduled with an attached session- parameter. The session is
  unscheduled and the session-parameters removed so that the default session parameters should be
  used.
  On the first schedule, traceback is seen. The session is again unscheduled and scheduled for second
  time and a crash is seen.
  Conditions: The symptom is observed when using custom session-parameters for a session and then
  removing it. Then using the default session-parameters followed by scheduled and unscheduled
  twice.
  Workaround: Use either the default session-parameters or custom session- parameters. Do not toggle
  between both.

- CSCts11743
  Symptoms: A Cisco router acting as a Call Manager Express device may unexpectedly reboot due
  to stack corruption.
  Conditions: The symptom is observed if more than eight calls are being queued in a route point, and
  one agent transfers a call back to this route point’s queue.
  Workaround: From UCCX, set the limit of calls in the queue to eight.

- CSCts12366
  Symptoms: Memory may not properly be freed when malformed SIP packets are received on the
  NAT interface.
  Conditions: None
  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The
Base and Temporal CVSS scores as of the time of evaluation are 5/4.8:
ctor=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-2578 has been assigned
to document this issue. Additional information on Cisco’s security vulnerability policy can be found
at the following URL:

- CSCts16285
  Symptoms: The system may experience delays in updating multicast information on the line cards.
  MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time
  out. In the worst case, the line card may become disconnected if timeouts continue for a long period.
  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.
  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load
  could be due to noncritical processes.

- CSCts20102
  Symptoms: NVRAM may lose or corrupt after router comes up.
Conditions: The symptom is observed during stress testing.
Workaround: Use the `wr erase` and then the `wr memory` commands if NVRAM corruption occurs.

- **CSCts28315**
  Symptoms: A DHCP PD request does not accept a specific server.
  Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC: http://tools.ietf.org/html/rfc3633#section-10
  A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.
  Workaround: There is no workaround.

- **CSCts28462**
  Symptoms: snmp-server host 1.2.3.4 traps version 2c public nhrp is reported as snmp-server host 1.2.3.4 traps version 2c public ds3.
  Conditions: Unknown.
  Workaround: There is no workaround.

- **CSCts30143**
  Symptoms: CPE WAN Management Protocol (CWMP) function is not working on UC500 platforms.
  Conditions: The symptom is observed under normal operation.
  Workaround: There is no workaround.

- **CSCts33952**
  Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.
  Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.
  Workaround: There is no workaround.
  Symptoms: When configuring 6VPE, you may see prefix corruption. Advertised prefix is different than the one installed. RD value also changes as well.
  Conditions: The symptom is observed when configuring “vpnv6 address family”.
  Workaround: There is no workaround.

- **CSCts38291**
  Symptoms: When configuring 6VPE, you may see prefix corruption. Advertised prefix is different than the one installed. RD value also changes as well.
  Conditions: The symptom is observed when configuring “vpnv6 address family”.
  Workaround: There is no workaround.

- **CSCts39240**
  Symptoms: The `advertise` command is not available in BGP peer-policy templates.
  Conditions: This symptom is observed on Cisco router running Cisco IOS Release 15.2(01.05)T, Cisco IOS Release 15.2(00.16)S, Cisco IOS Release 15.1 (03)S0.3, or later releases.
Workaround: The keyword and functionality is still available to be configured in the BGP neighbor command.

- CSCt39535
  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.
  Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.
  Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.
  Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.
  Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCt49769
  Symptoms: Switch or router device crashes after critical authentication is unconfigured.
  Conditions: The symptom is observed when critical authentication is configured on an interface using the command:
  `authentication event server dead action reinitialize vlan ...`
  and then un-configured using either:
  `no authentication event server dead action authorize vlan ...`
  or
  `no authentication event server dead`.
  Workaround: Use the correct command to unconfigure critical authentication: `no authentication event server dead action reinitialize vlan ...`.

- CSCt55371
  Symptoms: OSPF will not flood link state updates over an interface. The command `show ip ospf flood-list` will show interface entries similar to:
  Interface Tunnel1, Queue length 181 Link state retransmission due in 1706165974 msec
  Note the high value for the retransmission timer.
  Conditions: The symptom is observed with some newer S and T releases including Cisco IOS Release 15.1(2)S, Release 15.1(3)S, and Release 15.2(1)T.
  The issue can occur on interfaces where OSPF has not flooded updates for more than 24 days. This can include interfaces that are newly configured for OSPF if the router has been up longer than that. Interfaces that flood LSAs at least once every 24 days will not be affected.
  Workaround: To clear a hung interface use `clear ip ospf process`.

- CSCt60981
  Symptoms: Watchdog timer tracebacks in common-flow-table code.
Caveats

Conditions: The symptom is observed when NBAR is turned on with IPv6 traffic with encrypted payload.
Workaround: There is no workaround.

- CSCts62082
Symptoms: Router generates the following message:

%NHRP-3-QOS_POLICY_APPLY_FAILED: Failed to apply QoS policy 10M-shape mapped to NHRP group xx on interface Tunnelxx, to tunnel x.x.x.x due to policy installation failure

Conditions: The symptom is observed when “per-tunnel” QoS is applied and there are more than nine DMVPN spokes. (Up to eight spokes, with QoS applied is fine.)
Workaround: There is no workaround.

- CSCts64539
Symptoms: The BGP next-hop is inaccessible. The show ip route command output in the global and VRF routing tables shows that the next-hop is reachable. The show ip bgp vpnv4 all attr next-hop command output shows max metric for the next-hop.
Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.
Workaround 1: If “set ip next-hop” is not configured in import route-map, this issue does not occur.
Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.
Workaround 3: If “neighbor x.x.x.x disable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCts69973
Symptoms: Spoke with 100 tunnels crashed at nhrp_process_delayed_resolution_event_wrapper.
Conditions: Source interfaces of the tunnels started to bring up.
Workaround: There is no workaround.

- CSCts71546
Symptoms: When a data client is authenticated first and then a voice client is authenticated, the traffic from the data client gets dropped.
Conditions: The symptom is observed in multi-auth and multidomain host modes when the dynamic VLAN for the voice client is different than the configured voice VLAN and the data client has to be authenticated first.
Workaround: Dynamic VLAN and configured VLAN for voice device should be same.

- CSCts86975
Symptoms: Spurious memory access and/or crash at cce_dp_csdb_api_classify.
Conditions: The symptom is observed when MACE (performance agent) has been configured.
Workaround: There is no workaround.

- CSCts98336
Symptoms: IKEv2 router crashes in exec when unconfiguring an active IKEv2 profile.
Conditions: The symptom is observed when an IKEv2 profile is in use. The crash is occurring only if the profile is configured in a certain way.
Workaround: Unconfigure first the AAA authorization block.

```
conf t
crypto ikev2 profile <profilename>
no aaa authorization group <type> list <AAA list name> name-mangler <Mangler name>
no crypto ikev2 profile <profilename>
```

- CSCtt03187
  Symptoms: CISP sub-systems are missing and the `cisp enable` CLI is not found.
  Conditions: The CISP enable feature is not found on the Cisco 3945E platform.
  Workaround: There is no workaround.

Further Problem Description: While making a comparison between the dx_mrvl code and the esw_mrvl code where the hwidb was being initialized it was found in the esw_mrvl case the initialization of the hwidb was taking place irrespective of the check on interesting, igmp or dot1x packet. In the case of dx_mrvl case the initialization of the hwidb was taking place on the condition of else. Thus the initialization in case of dx_mrvl within else condition was not reasonable because hwidb should be initialized irrespective of packet type.

- CSCtt04168
  Symptoms: Tearing down one of the authenticated sessions will clear the mac-address of the other authenticated session.
  Conditions: This symptom is observed in multidomain authentication (MDA) and multi-auth host mode.
  Workaround: The only workaround is to change the host mode to multi-host.

- CSCtt07525
  Symptoms: Spoke router may crash when NHRP is cleared on another spoke.
  Conditions: The symptom is observed with FlexVPN and with spoke-to-spoke tunnels.
  Workaround: There is no workaround.

- CSCtt10507
  Symptoms: When data and voice clients are authenticated and then voice client session is cleared, data session traffic is blocked.
  Conditions: The symptom is observed in multi-auth and multi-domain host modes when the dynamic VLAN for the voice client is different than the configured voice VLAN.
  Workaround: Dynamic VLAN and configured VLAN for voice device should be same.

- CSCtt10633
  Symptoms: Tearing down the voice authenticated session will clear the mac-address of other authenticated data sessions.
  Conditions: This symptom is observed in multidomain authentication (MDA) and multi-auth host mode.
  Workaround: There is no workaround.

- CSCtt11996
  Symptoms: When Open Access is enabled and the port is unauthorized and is in authz fail state, a traffic drop is observed for about 20 secs as soon as the restart timer kicks in.
  Conditions: This symptom is observed when Open Access is enabled.
  Workaround: Enable “spanning-tree portfast”.
- **CSCtt14448**
  Symptoms: Traceback seen at esw_mrvl_mat_oper_enqueue_msg.
  Conditions: The symptom is observed on a UUT loaded with the Cisco 15.2(1.13) T image.
  Workaround: There is no workaround.
  Further Problem Description: The traceback was seen because of no process to handle MAT operation related functions in esw_mrvl_portdriver_subsys_init initialization.

- **CSCtt14867**
  Symptoms: Wake on LAN (WoL) is not able to wake up the PC.
  Conditions: This symptom is observed in multidomain authentication (MDA) and single-host host modes.
  Workaround: There is no workaround.

- **CSCtt15061**
  Symptoms: Router crashes after few hours when two copper cards are installed on the router.
  Conditions: The symptom is observed when two copper (SHDSL-EA) cards are installed on a single router.
  Workaround: There is no workaround.

- **CSCtt20215**
  Symptoms: Controller down after reload.
  Conditions: The symptom is observed with a VWIC3 E1/CAS connected to a PBX.
  Workaround: Need to unplug/plug the cable or reset link from PBX side.

- **CSCtt33158**
  Symptoms: If WRED is already present and the queue limit is configured in packets then WRED thresholds become 0.
  Conditions: The symptom is observed if WRED is already present and the queue limit is configured in packets.
  Workaround: Remove WRED and reattach it.

- **CSCtt37564**
  Symptoms: dACL is not working.
  Conditions: The symptom is observed under all conditions. The IP is not learnt for the first host resulting in ACLs never being applied.
  Workaround: Will work in multi-auth environments.

- **CSCtt43843**
  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.
  Conditions: It is occurring with a Cisco 7200 platform loaded with the 15.2 (1.14)T0.1 image.
  Workaround: There is no workaround.

- **CSCtt44337**
  Symptoms: A Cisco 2911 crashes multiple times after an upgrade.
Conditions: Crashes are encountered on the Cisco 2911 after an upgrade to Cisco IOS Release 15.2(1)T1 to support the SCANSAFE functionality. The crashes are due to reviving TCP packets out of order.

Workaround: There is no workaround.

- CSCtt45536
  Symptoms: “FlowVar- Chunk malloc failed” messages are seen and this may be accompanied by slow console response.
  Conditions: The symptom is observed when a mix of IPv4 and IPv6 traffic is going through the router configured with QoS, VM, etc.
  Workaround: There is no workaround.

- CSCtu11467
  Symptoms: A “clear auth session mac <data-mac>” is not triggering new authentication for MAB clients.
  Conditions: The symptom is observed when the configured and downloaded data VLAN are different.
  Workaround: Configure the same VLAN in switch and ACS.

- CSCtu12162
  Symptoms: When data and voice client are authenticated and then the voice client session is cleared, (two or more times), the voice mac is not learnt back and the voice authentication session does not start.
  Conditions: The symptom is observed in multi-auth and multi-domain hostmodes
  Workaround: Dynamic VLAN and configured VLAN for voice device should be same.

- CSCtu16809
  Symptoms: Deny entries in the KS ACL are not downloaded to the GM when the GM has an ISM VPN card.
  Conditions: The GM is using an ISM VPN card.
  Workaround: Use deny entries on a local ACL on the GM, or disable the ISM VPN.

- CSCtu17987
  Symptoms: When a dot1x PC is rebooted, EAPOL packets are not reaching the CPU. Authentication of the PC fails.
  Conditions: Observed in MDA mode.
  Workaround: Once the dot1x is failed, clear the session by issuing `clear auth sess interface`. 

Caveats for Cisco IOS Release 15.2(1)T

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in this section.

In this section, the following information is provided for each caveat:

- **Symptoms**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This document contains the following sections:

- **Resolved Caveats**—Cisco IOS Release 15.2(1)T4, page 452
- **Resolved Caveats**—Cisco IOS Release 15.2(1)T3a, page 457
- **Resolved Caveats**—Cisco IOS Release 15.2(1)T3, page 458
- **Resolved Caveats**—Cisco IOS Release 15.2(1)T2, page 480
- **Resolved Caveats**—Cisco IOS Release 15.2(1)T1, page 496
- **Open Caveats**—Cisco IOS Release 15.2(1)T, page 506
- **Resolved Caveats**—Cisco IOS Release 15.2(1)T, page 531
Resolved Caveats—Cisco IOS Release 15.2(1)T4

- CSCtj10515
  Symptoms: Crash seen in IGMP input process.
  Conditions: The symptom is observed in a multi-VRF scenario with extranet MVPN.
  Workaround: There is no workaround.

- CSCtj95182
  Symptoms: Scanning for security vulnerabilities may cause High CPU condition on Cisco Catalyst 3750.
  Conditions: Network scanner run against a 3750 running 12.2.55.SE.
  Workaround: There is no workaround.
  Additional Information: Vulnerable versions:
  - 12.2(52)EX through 12.2(55)SE4
  - 15.1(3)T through 15.1(4)XB8a
  - 15.2(1)GC - 15.2(3)XA
  First fixed in: 12.2(55)SE5, 15.0(1)EX, 15.1(1)SG, 15.2(1)E, 15.2(4)M, 15.3(1)T.
  In the meantime, Cisco published several security advisories for Smart Install vulnerabilities:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smart-install

- CSCtq14253
  Symptoms: Joins/registers not forwarded to the RP when first configured.
  Conditions: The symptom is observed when the router is first configured.
  Workaround: Reload all routers in the setup.

- CSCts08224
  Symptoms: Expected ACL/sessions not found for most of the protocols.
  Conditions: The symptom is observed with expected ACL/sessions.
  Workaround: There is no workaround.

- CSCtt43552
  Symptoms: A Cisco router reloads with the warm-reboot command.
  Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.
  Workaround: There is no workaround. Remove “warm-reboot” from configuration (router will not be able to use warm reboot feature).

- CSCtu08373
  Symptoms: Router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.
  Conditions: IOS firewall is configured and traffic is flowing through the router.
  Workaround: There is no workaround.
- **CSCtu28696**
  Symptoms: A Cisco ASR 1000 crashes with `clear ip route *`.
  Conditions: The symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, then clear the configuration.
  Workaround: There is no workaround.

- **CSCtw78539**
  Symptoms: A Cisco ISR router running Cisco IOS Release 15.2(2)T may lose the ability to forward traffic via its Gigabit Ethernet interface due to a stuck Tx ring.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T, 15.2(2)T, and 15.2(4)M. This is a regression issue that does not affect 15.0(1)M3 nor 15.1(4)M2 based on anecdotal accounts.
  During the event the following logs can be seen which indicate a spurious memory access has occurred:

    %ALIGN-3-SPURIOUS: Spurious memory access made at 0xXXXXXXXX reading 0x0
    %ALIGN-3-TRACE: -Traceback= 0xXXXXXXXX ...
  At this time, the Tx ring of the interface becomes hung, causing packet drops to accumulate at the output queue (as seen via “show interface”), effectively preventing traffic flow. E.g.:
  
  Total output drops: 25185
  Output queue: 331/1000/25184 (size/max total/drops)
  Workaround: Reload the router or bounce the interface via “shut”/”no shut”.

- **CSCtx56174**
  Symptoms: Cisco router hangs until a manual power cycle is done. If the `scheduler isr-watchdog` command is configured, the device will crash and recover instead of hanging until a power cycle is done.
  Conditions: This is seen with websense URL filtering enabled and with zone based firewalls.
  Workaround: Disable URL-based filtering.

- **CSCtz35999**
  Symptom: The Cisco IOS Software Protocol Translation (PT) feature contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.
  Cisco has released free software updates that address this vulnerability.
  Workarounds that mitigate this vulnerability are available.
  This advisory is available at the following link:
  
  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.
  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:
  

- **CSCtz42421**
  Symptoms: The device experiences an unexpected crash.
Caveats for Cisco IOS Release 15.2(1)T

Conditions: This symptom is observed when Zone-Based Firewalls are enabled. H225 and H323 inspection is being done during the crash. The actual conditions revolving around the crash is still being investigated.

Workaround: There is no workaround.

- **CSCtz58941**
  
  Symptoms: The router crashes when users execute the `show ip route XXXX` command.
  
  Conditions: This symptom is observed during the display of the `show ip route XXXX`, when the next-hops of “XXXX” networks are removed.
  
  Workaround: The `show ip route XXXX` command (without “XXXX”) does not have the problem.

- **CSCtz71084**
  
  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.
  
  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

  CE0--------PE0--------RR || PE0--------PE1--------CE0
  
  Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.
  
  This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: `no network x.x.x.x mask y.y.y.y`
  
  Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.
  
  Workaround: Hard clear.

- **CSCua12317**
  
  Symptoms: The Cisco 3900 router resets when configuring Object Group/ACL when there is traffic on the interface where an ACL match is needed.
  
  Conditions: This symptom is observed with the following conditions:
  
  1. The ACL definition should have service OG ACE.
  2. Reconfigure the service OG ACE or delete it.
  3. Traffic should be passing on the interface where the OG is applied when the above operation is performed.
  
  Workaround:
  
  1. Configure a new ACL with the changes needed and apply it to the interface of interest, instead of modifying the already applied one. This is recommended when configuration change is needed.
  2. Remove ACL checks on the interface when changing the configuration (“no ip access-group.”).

- **CSCua15292**
  
  Symptoms: Router may crash unexpectedly with crypto in running-configuration.
Conditions: The symptom is observed with a router running at normal operation. When it crashes, the error message below is found in the crashinfo file:

```
%CRYPTO-4-RECV_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=172.8.9.8, prot=50, spi=0xE8FB045F(3908764767), srcaddr=10.0.100.1, input
interface=GigabitEthernet0/0
```

Workaround: There is no workaround.

- **CSCua39390**

  Symptoms: The PRI configuration (voice port) is removed after a reload:

  ```
  interface Serial1/0:23          ^
  % Invalid input detected at '^' marker.
  no ip address
  % Incomplete command.
  encapsulation hdlc
  % Invalid input detected at '^' marker.
  isdn incoming-voice voice
  % Invalid input detected at '^' marker.
  no cdp enable
  % Invalid input detected at '^' marker.
  voice-port 1/0:23
  % Invalid input detected at '^' marker.
  Also getting trace back:
  ```

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T and Release 15.1(4)M4. The issue is not occurring with Cisco IOS Release 12.4(24)T6 or lower. The issue occurs after reload.

  Workaround: Reapply configuration after router comes back up.

- **CSCua40273**

  Symptoms: The ASR1k crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the ASR1K with version 15.1(02)S software.

  Workaround: Avoid changing the VRF while querying for MIB information.

- **CSCua55629**

  Symptoms: SIP memory leak seen in the event SIPSPI_EV_CC_MEDIA_EVENT.

  Conditions: The command `show memory debug leaks` shows a CCSIP_SPI_CONTORL leak with size of 6128 and points to the event “SIPSPI_EV_CC_MEDIA_EVENT”: 

  Adding blocks for GD...

  ```
  I/O memory
  Address Size Alloc_pc PID Alloc-Proc Name
  Processor memory
  ```

  ```
  Address Size Alloc_pc PID Alloc-Proc Name
  ```
Caveats for Cisco IOS Release 15.2(1)T

CSCua99969
Symptoms: IPv6 PIM null-register is not sent in the VRF context.
Conditions: This symptom occurs in the VRF context.
Workaround: There is no workaround.

CSCub55790
The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. Affected devices that are configured as Smart Install clients are vulnerable.
Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.
This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-smartinstall

CSCuc07799
Symptoms: The router crashes while booting with Cisco IOS Release 15.2(4)M weekly images.
Conditions: This symptom occurs when the ISM-VPN Module is inserted in the router. WCCP and RG-Infra features are also enable.
Workaround: There is no workaround.

CSCuc67033
Symptoms: A Cisco IOS router with the ISM VPN encryption module enabled can experience memory corruption-related crashes.
Just before the crash, the router may display some syslog error messages related to the ISM VPN module:
Aug 21 15:55:22: !!! Cannot find Revt counters struct for flowid: 0x4400012A
Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A
Aug 21 15:55:24: !!! Cannot find Revt counters struct for flowid: 0x4400012A

Here, the word “Revt” is specific for the ISM VPN module.

Also, some generic syslog error messages related to memory allocation failures may be displayed the crash:

Aug 21 15:55:33: %SYS-3-BADBLOCK: Bad block pointer DD7D7D0
   - Traceback= 23B9EA7Cz 23BA1A44z 23BA1E24z 23B712B8z 23B7129Cz
   352791C4,22DB4A50 352791C4,3000006C 38808760,2627EDF0 34C91824,262724A8
   352791C4,22DB6214 352791C4,22DB4A50 352791C4,3000006C 352791C4,22DB6214
   352791C4,22DB4A50 352791C4,3000006C 352791C4,22DB6214 3875D9C4,600002CA
   3875D5E0,2627EDF0 35092ACC,262724A8 352791C4,22DB4A50 352791C4,3000006C
Aug 21 15:55:33: %SYS-6-BLKINFO: Corrupted next pointer blk DD7D7D0, words 32808, alloc 2148636C, InUse, dealloc 0, rfcnt 1

Conditions: This symptom is observed with the following conditions:

- The ISM VPN crypto acceleration module is installed, enabled, and used for crypto operations (IPsec, etc.).
- Cisco IOS supports ISM VPN (Cisco IOS Release 15.2(1)T1 or later releases).

Workaroud: Disable the ISM VPN module. The crash is specific to ISM VPN.

- CSCuc82992

Symptoms: The router crashes upon execution of “no crypto engine slot 0”, when RG-infra feature is enabled.

Conditions: This symptom occurs when RG-Infra and ISM-VPN are configured and when issuing “no crypto engine slot 0”.

Workaround: There is no workaround.

- CSCud02361

Symptoms: Sequence number of spoofed ACK sent to the server has a 0x00 value.

Conditions: Once the max-incomplete high is reached, when the next SYN packet is sent from the client, the UUT sends a SPOOFED-ACK after getting the SYN-ACK from the server. When this ACK packet is observed at the server pagent with the packets tool, the sequence number is found to be 0x00.

Workaround: There is no workaround.

- CSCue94880

Symptoms: RTP traffic fails in reverse direction when an outside source list is configured and RTP SA IP matches against this list.

Conditions: The symptom is observed with a Cisco IOS version above 12.4(9) mainline.

Workaround: Use Cisco IOS Release 12.4(9).

Resolved Caveats—Cisco IOS Release 15.2(1)T3a

Cisco IOS Release 15.2(1)T3a is a rebuild release for Cisco IOS Release 15.2(1)T. The caveats in this section are resolved in Cisco IOS Release 15.2(1)T3a but may be open in previous Cisco IOS releases.

- CSCub16372
Caveats

Symptoms: In extremely rare cases, Cisco ISR-G2 cannot boot up with certain ROMMON versions with the error “Signature did not verify”.

So far, only one image is found to have this problem: c3900-universalk9-mz.SPA.152-1.T3.bin.

Conditions: The issue will happen when the following conditions are met at the same time:

1. The platform is affected.
2. The ROMMON version running at the router is within the affected ROMMON version range.
3. The first calculated hash value is 0 during the Cisco IOS image building process.

Since it is extremely rare that the third condition will happen, so far only one image is found to have this problem.

Workaround: There is no workaround.

Upgrading ROMMON to the latest version of Cisco IOS 15.0(1r)M16 or 15.1(1r)T5 will fix the issue completely.

The ROMMON upgrade can be done using one single CLI command in the router’s enable mode:

Router# upgrade rom-monitor file flash:<ROMMON_file_name>

<ROMMON_file_name> is the ROMMON file name for the specific platform that is downloadable from cisco.com. For example, C3900_RM2.srec.SPA.150-1r.M16 is the latest ROMMON version for Cisco C39xx platforms located at the cisco.com download site:


Resolved Caveats—Cisco IOS Release 15.2(1)T3

Cisco IOS Release 15.2(1)T3 is a rebuild release for Cisco IOS Release 15.2(1)T. The caveats in this section are resolved in Cisco IOS Release 15.2(1)T3 but may be open in previous Cisco IOS releases.

- CSCtj48387
  Symptoms: After a few days of operation, a Cisco ASR router that is running as an LNS box, crashes with DHCP related errors.
  Conditions: This symptom occurs when DHCP enabled and sessions get DHCP information from a RADIUS server.
  Workaround: There is no workaround.
  Further Problem Description: This fix needs to be included in the Cisco ME 3400.

- CSCtl73132
  Symptoms: Router may crash and reset when the show ipc hog- info or show tech-support ipc commands are run repetitively on either the switch processor or route processor.
  Conditions: The issue can be seen when the show ipc hog- info or show tech-support ipc commands are run repetitively on either the switch processor or route processor.
  Workaround: Do not use the show ipc hog- info or show tech-support ipc commands.

- CSCtl90292
  Symptoms: The following error messages are displayed:

  an 18 08:00:16.577 MET: %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes failed from 0x42446470, alignment 32
  Pool: I/O  Free: 11331600  Cause: Memory fragmentation Alternate Pool: None
Caveats for Cisco IOS Release 15.2(1)T

OL-25471-04 Rev. P0

Caveats

Free: 0  Cause: No Alternate pool -Process= "BGP I/O", ipl= 0, pid= 564
-Traceback= 417E8BEC 4180FA6C 42446478 42446B64 42443984 40FC18C8 40FCCB4C
40FD1964 403BDBFC 403BCC34 40344508 403668AC

Show buffers shows:

1. Increased miss counters on the EOBC buffers.

2. Medium buffer leak

   Router#sh buffers
   Buffer elements:
   
   779 in free list (500 max allowed)
   1582067902 hits, 0 misses, 619 created

   Interface buffer pools:
   
   ....
   
   Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @ 00:01:17):
   
   273 in free list (64 min, 3000 max allowed)
   
   EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
   
   0 in free list (0 min, 2400 max allowed)
   2400 hits, 161836 fallbacks
   1200 max cache size, 129 in cache
   
   ....

   Conditions: This symptom is observed when several hits and failures are seen for medium buffers.
   All are linktype IPC. For example:

   Buffer information for Medium buffer at 0x4660E964
   
   ....
   
   linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rtype 0
   if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)

   Also, “show buffers old” shows some buffers hanging on on EOBC buffers list for really long time
   like weeks or more.

   Workaround: There is no workaround.

   • CSCtn04357

   Symptoms: When applying the following netflow configuration in the same sequence, the standby
   supervisor module continuously reloads:

   vlan configuration 161
   ip flow monitor flowmonitor1 in
   ip flow monitor flowmonitor1 input
Caveats for Cisco IOS Release 15.2(1)T

Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

Workaround 1: Remove the flow monitor configuration.
Workaround 2: Use netflow-v9 export protocol.
Workaround 3: Use a record format exportable by netflow-v5.

- CSCtn07696
  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the show tech-support command output using the ftp command due to TCP-2-INVALIDTCB.
  Conditions: This symptom is observed with the following CLI:
  `show tech-support | redirect ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt`
  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.
  Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn59075
  Symptoms: A router may crash.
  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible Netflow needs to be running.
  Workaround: Disable Flexible NetFlow on all interfaces.

- CSCtn65116
  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.
  Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Release 12.2(33)SRB or later. Earlier versions are not affected. This occurs with the same prefixes with different mask lengths, e.g.: 10.0.0.0/24 and 10.0.0.0/26 (but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1). It is seen with the following process:
  1. Assume the prefix, 10.0.0.0/24, is imported from VPNv4 to VRF. It has been allocated a label of 16.
  2. The allocated label changes from 16 to 17, e.g.: due to interface flapping or BGP attribute change.
  3. However, before the BGP import happens, a more specific prefix (e.g.: 10.0.0.0/26) is added to the BGP radix tree, but it is denied for importing due to, say, RT policy.
  Workaround: Remove RT or import map and add it back. Note, however, that if the above conditions occur again, the issue could reappear.

- CSCto09059
  Symptoms: CPUHOG at IPC Check Queue Time Process results in IOSD crash.
  Conditions: This symptom occurs with multiple RP switchovers with ISG PPPoE sessions.
  Workaround: There is no workaround.

- CSCOto70391
  Symptoms: Under policy-map when bandwidth CLI is removed and switch-over, the standby reboots continuously.
Caveats for Cisco IOS Release 15.2(1)T

OL-25471-04 Rev. P0

Caveats

- CSCto77352
  Symptoms: Standby cannot reach HOT sync state with active. Standby RP will keep resetting. The following messages are printed:
  %SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1), process = IPC Dynamic Cache.
  Conditions: This symptom occurs with SSO mode when a Cisco ASR 1000 series router is configured with ISG as DHCP server and with low DHCP lease timer.
  Workarounds: There is no workaround.

- CSCtq14817
  Symptom: Traceback or crash might happen when PPTP related traffics were passing through NAT configured device.
  Conditions: A race condition when PPTP packets were subjected to NAT, that might cause NAT to behave improperly and cause the issue.
  Workarounds: There is no workaround.

- CSCtq20168
  Symptoms: Chunk leak is seen at ipc_init_message_system.
  Conditions: This symptom is seen with the test ipc port send 0 0 rpc type 0 1 1 command.
  Workarounds: There is no workaround.

- CSCtq24557
  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.
  Conditions: The symptom is observed in a large scale scenario.
  Workarounds: There is no workaround.

- CSCtq49325
  Symptoms: Router reloads when a graceful shutdown is done on EIGRP.
  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.
  Workarounds: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.
  Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. If a particular path is threaded to be sent - in this case it is scheduled for a reply message - the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to
Caveats for Cisco IOS Release 15.2(1)T

Caveats

- **CSCtq57742**
  Symptoms: Router crashes for corrupted chunk memory when BGP neighbor is shutdown.
  Conditions: This symptom is seen with BGP and IPv6 configuration.
  Workaround: There is no workaround.

- **CSCtq59923**
  Symptoms: OSPF routes in RIB point to an interface that is down/down.
  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.
  Workaround: Configure “ip routing protocol purge interface”.

- **CSCtq60703**
  Symptoms: The device crashes and traceback is seen when executing **write network**.
  Conditions: The symptom is observed when the command **write network** is used with no URL specified.
  Workaround: Specify a URL.

- **CSCtq77024**
  Symptoms: Metrics collection fails on hop0 if route change event occurs.
  Conditions: This symptom is observed when the mediatrace is not passing up an interface type that is acceptable to DVMC when a route change occurs on the node which has the initiator and responder enabled.
  Workaround 1: Remove and reschedule mediatrace session.
  Workaround 2: Remove and reconfigure mediatrace responder.

- **CSCtq85564**
  Symptoms: The fix of CSCto77352 may cause a data corruption problem.
  Conditions: This symptom is seen when two processes are calling the same function that is raising the race condition.
  Workaround: There is no workaround.

- **CSCtq85728**
  Symptoms: An EHWIC-D-8ESG card is causing an STP loop.
  Conditions: EHWIC-D-8ESG might not be blocking appropriate ports according to calculated STP topology that introduces the loop in the network.
  Workaround: There is no workaround.

- **CSCtq91305**
  Symptoms: Standby cannot reach HOT sync state with active. The standby RP keeps resetting. The following message is displayed:
%SYS-3-CPUHOG: Task is running for (3305)msecs, more than (2000)msecs (1/1), process = IPC Dynamic Cache.

Conditions: This symptom occurs with SSO mode, when the Cisco ASR1k is configured with ISG as DHCP server and with a low DHCP lease timer.

Workaround: There is no workaround.

- CSCtq97883
  Symptoms: Traceback is shown. The root cause is a null pointer.
  Conditions: The symptom is observed during longevity testing of Cisco IOS Release 12.4(24)GC3a and Release 15.1(2)GC.
  Workaround: There is no workaround.

- CSCtr45287
  Symptoms: Router crashes in a scale DVTI scenario.
  Conditions: The symptom is observed when the IPsec tunnel count reaches around 2500.
  Workaround: Use fewer tunnels or use a different platform.

- CSCtr46123
  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.
  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.
  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

- CSCtr53944
  Symptoms: IPv6 unicast packets are dropped.
  Conditions: The symptom is observed when there is a breakage in VMI fastpath when passing IPv6 unicast packets.
  Workaround: There is no workaround.

- CSCtr54327
  Symptoms: A Cisco router may crash due to a SegV exception or may have spurious access when a fax comes in.
  Conditions: This symptom is observed on a voice gateway that is configured with transcoding and fax passthrough. When a fax call comes in for a codec, but is not configured for a codec, then the “a=silenceSupp:off” option is set in SDP.
  Workaround: Disable fax by going into the “voice service voip” mode and configuring the fax protocol none command.

- CSCtr58140
  Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.
  Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.
  Workaround: There is no workaround.
CSCtr86328
Symptoms: A device that is running Cisco IOS might reload when the web browser refreshes or reloads the SSL VPN portal page.
Conditions: This symptom is observed on a Cisco IOS device that is configured for clientless SSL VPN.
Workaround: There is no workaround.

Further Problem Description: This problem has been seen when the stock Android browser visits the SSL VPN portal (after authentication) and refreshes (reloads) the page. However, the issue is not browser-specific and other browsers might trigger the issue too.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/6.5:
CVE ID CVE-2012-1344 has been assigned to document this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:

CSCtr88739
Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.
Symptom 2: The routes in BGP may not get installed to RIB.
Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for symptom 1: Remove “import-route target” and reconfigure route-target.
Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

CSCtr92202
Symptoms: Compilation failure is seen with version gcc.c4.2.1.
Conditions: This symptom occurs when compiling images using gcc.c4.2.1.
Workaround: There is no workaround.

CSCts03251
Symptoms: A Cisco 2921 router running Cisco IOS Release 15.1(4)M with the “logging persistent” feature configured may crash.
Conditions: This symptom is observed with the “logging persistent” feature.
Workaround: Disable the “logging persistent” feature.

CSCts31111
Symptoms: Coredump generation fails on the Cisco 800.
Caveats for Cisco IOS Release 15.2(1)T

Conditions: This symptom occurs when coredump is configured.
Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:
```
conf t
config-reg 0x0
end
wr
reload
yes
<rommon prompt>
DISABLE_WATCHDOG=yes
sync
set
config-reg 0x2102
reset
```

- **CSCts56044**
  
  Symptoms: A Cisco router crashes while executing a complex command. For example:
  
  ```
  show flow monitor access_v4_in cache aggregate ipv4 precedence sort highest ipv4 precedence top 1000
  ```
  
  Conditions: This symptom is observed while executing the `show flow monitor top` top-talkers command.
  
  Workaround: Do not execute complex flow monitor top-talkers commands.

- **CSCts65564**
  
  Symptoms: In a large scale DMVPN environment, a DMVPN hub router may crash in the Cisco IOS process under high scale conditions.
  
  Conditions: This only occurs if CRL caching is disabled (with the command `crl cache none` under the pki trustpoint configuration).
  
  Workaround: Enable CRL caching (this is the configured default).

- **CSCts68541**
  
  Symptoms: In IPsec scaling test, when CPE is keeping reload, all IPsec sessions will be torn down and reestablished. During the session flapping, RP reset is observed sometimes.
  
  Conditions: This symptom is seen with CPE reloading continually.
  
  Workaround: There is no workaround.

- **CSCts70790**
  
  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.
  
  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.
  
  Workaround: Remove and re-add the `neighbor default-originate` command on the Cisco 7600 router and do a soft clear for the VRF neighbor.
• CSCts72911
Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the non-restarting peer (RR, in this case).
Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.
Workaround: There is no workaround.

• CSCtt02313
Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.
Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.
Workaround: There is no workaround.

• CSCtt26074
Symptoms: Memory leak with IP SLAs XOS Even process.
Conditions: The symptom is observed with IP SLA configured.
Workaround: There is no workaround.

• CSCtt26692
Symptoms: Router crashes due to memory corruption. In the crashinfo you may see:
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxx data
xxxxxxxxxx chunkmagic xxxxxxxx chunk_freemagic EF4321CD -
Process= "CCSIP_SPI_CONTROL", ipl= 0, pid= 374
chunk_diagnose, code = 1
chunk name is MallocLite

Conditions: Router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.
Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

• CSCtt26721
Symptoms: A Cisco router may see increased CPU utilization when NBAR is used.
Conditions: This has been experienced on a Cisco 3925 router running Cisco IOS Release 15.1(3)T2.
Workaround: There is no workaround.

• CSCtt37516
Symptoms: Line card crash with priority traffic when QoS policy is applied. The defect impacts the distributed system, 7600, with line card using software data plane implementation, Enh Flex or SIP200, when priority feature is enable with mlppp/mlpFR interleaving.
Conditions: The symptom is observed with the QoS priority feature. When interleaving is enabled, add/remove/modify priority feature will trigger this defect with live traffic.
Workaround: There is no workaround.

- CSCtu32301
  Symptons: Memory leak may be seen.
  Conditions: This is seen when running large show commands like show tech-support on the line card via the RP console.
  Workaround: Do not run the show commands frequently.

- CSCtu40028
  Symptons: The SCHED process crashes.
  Conditions: The issue occurs after initiating TFTP copy.
  Workaround: There is no workaround.

- CSCtv21900
  Symptons: Intermittent one-way audio occurs from an MGCP gateway to a Cisco IP phone.
  Conditions: This symptom is observed under the following conditions:
  - Encrypted call with SRTP
  - MGCP Controlled Gateway
  - Cisco IOS Release 15.1(4)M or later releases
  Phone logs show the following message:
  The “Rcvr Lost Packet” counter on the Cisco IP phone begins to increment as soon as the call connects.
  Workaround 1: Downgrade the software to Cisco IOS Release 15.1(3)T or earlier releases.
  Workaround 2: Perform a hold/resume on the one-way audio call. This mitigates the problem.

- CSCtv36812
  Symptons: Incorrect crashInfo file name is displayed during crash.
  Conditions: The symptom is observed whenever a crash occurs.
  Workaround: There is no workaround.

- CSCtw45055
  Symptons: A Cisco ASR router may experience a crash in the BGP scheduler due to a segmentation fault, if BGP dynamic neighbors have been recently deleted due to link flap. For example:
  %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
  %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time expired) x bytes
  %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification received
Caveats

Caveats for Cisco IOS Release 15.2(1)T

%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session Neighbor deleted

%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast
topology base removed from session Neighbor deleted

%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

Exception to IOS Thread:
Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler

The scheduler process will attempt to reference a freed data structure, causing the system to crash.
Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.
Workaround: There is no workaround.

- CSCtw45592
  Symptoms: The ntp server DNS-name command is not synced to the standby. When the no ntp server hostname command is issued later on the active, the standby reloads because the configuration was not added.
  Conditions: When the device is reloaded or when the DNS name is not resolved, the configuration is not added. It is seen after the standby sync failure, then issuing the no ntp server hostname.
  Workaround: Use IP/IPv6 addresses instead of the hostname for NTP configurations. The IP/IPv6 address can be found by pinging the hostname.

- CSCtw46229
  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.
  Conditions: The symptom is observed with PPP negotiations and the session involving PPPoA.
  Workaround: Ensure all your PPP connections stay stable.

- CSCtw55976
  Cisco IOS Software contains a vulnerability in the Intrusion Prevention System (IPS) feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist.
  Cisco has released free software updates that address this vulnerability.
  Workarounds that mitigate this vulnerability are available.
  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ios-ips

- CSCtw61872
  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.
  Conditions: The symptom is observed when executing a complex sort with top-talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):
sh flow monitor QoS_Monitor cache sort highest counter packets top 1000 sh flow monitor QoS_Monitor cache sort highest counter packets top 10000

Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw62310
  
  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service- policy”.
  
  Conditions: The symptom is observed when removing the policy-map from map-class.
  
  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw71564
  
  Symptoms: Not all data packets are accounted for in the “show stats” output of the video operation.
  
  Conditions: The symptom is observed with heavy load on the responder caused either by many video sessions or other processes.
  
  Workaround: Reduce processor load on device running the responder.

- CSCtw84664
  
  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.
  
  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerability.
  
  This advisory is available at the following link:
  
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip

- CSCtw88094
  
  Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.
  
  Conditions: This symptom occurs shortly after the “ip sla schedule X start specific_start_time” command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.
  
  Workaround: Unschedule the probe before rescheduling for a specific start time.

- CSCtx01604
  
  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.
  
  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.
  
  Workaround: Do not use any dynamic network interface IP address as CNS ID.
• CSCtx19332
Symptoms: A Cisco router crashes when “remote mep” is unlearned while auto EOAM operations are executing.
Conditions: This symptom is observed if “remote mep” is unlearned from the auto database (shutdown on interface or remote mep reload) while the “IP SLA ethernet-monitor jitter” operation is still running. The crash occurs if the initial control message times out.
Workaround: There is no workaround.

• CSCtx29543
Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when doing the show ip route command.
Conditions: This symptom occurs under the following conditions:
1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exist.
2. A default route exists.
3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.
The router may now crash when doing show ip route command or when default route is updated.
Workaround: There are two possible workarounds:
1. Insure that not all 23 supernet mask lengths are populated by doing route filtering.
2. If workaround #1 is not possible, then insure that at least one supernet route for all possible mask lengths exists at all times, for example by configuring summary routes that do not interfere with normal operation.

• CSCtx32329
Symptoms: When using the show ipv6 rpf command, the router crashes or displays garbage for RPF idb/nbr.
Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.
Workaround: Do not use static multicast routes, or make sure that the next hop specified can always be resolved. Do not use the show command.

• CSCtx32628
Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.
Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:
- BGP full mesh is configured.
- BGP cluster-id is configured.
- address family vpnv4 is enabled.
- address family ipv4 mdt is enabled.
- The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.
Workaround: Remove the cluster-id configuration or hard-reset the BGP session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.
• CSCtx38806
 symptoms: SSL VPN users lose connectivity as soon as Windows machine gets updated with security update KB2585542. This affects Cisco AnyConnect clients and may also affect IE browsers.

This can affect any browser that has the BEAST SSL vulnerability fix, which uses SSL fragmentation (record-splitting). (Chrome v16.0.912 browser is affected for clientless WebVPN on Windows and MAC.)

The problem affects Firefox also (version 10.0.1) displaying the following message:

"The page isn’t redirecting properly"

Conditions: This symptom is observed on Cisco IOS that is acting as head end for SSL VPN connections.

Workaround: Any of the following workarounds will work:

1. Use the clientless portal to start the client. This only works in some versions of Cisco IOS.
2. Uninstall the update.
3. Use rc4, which is a less secure encryption option. If this meets your security needs, then you may use it as follows:

   ```
   webvpn gateway gateway name
   ssl encryption rc4-md5
   ```

4. Use AC 2.5.3046 or 3.0.3054.
5. Use older versions of Firefox (9.0.1).

Further Problem Description: For AnyConnect users, the following user error message is seen:

"Connection attempt has failed due to server communication errors. Please retry the connection"

The AnyConnect event log will show the following error message snippet:

Function: ConnectIfc::connect
Invoked Function: ConnectIfc::handleRedirects
Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED

PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:


• CSCtx51935

Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

Conditions: The symptom is observed with the following steps:

```
interface gi1/2
mpls traffic-eng tunnels
no shut
```

```
router OSPF 1
mpls traffic-eng area 100
```
mpls traffic-eng router-id lo0
end

show mpls traffic-eng link-management summary

Workaround: There is no workaround.

- **CSCtx56174**
  Symptoms: Cisco router hangs until a manual power cycle is done. If the scheduler `isr-watchdog` command is configured, the device will crash and recover instead of hanging until a power cycle is done.
  Conditions: This is seen with webspense URL filtering enabled and with zone based firewalls.
  Workaround: Disable URL-based filtering.

- **CSCtx57784**
  Symptoms: Device crashes while configuring “logging persistent url”.
  Conditions: Occurs when the destination file system has zero free bytes left.
  Workaround: There is no workaround.

- **CSCtx66804**
  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.
  Conditions: The symptom is observed with the following conditions:
  - “ppp lcp delay 0” is configured.
  - The symptom can be seen on Cisco IOS Release 15.0(1)M5.
  Workaround: Set delay timer without 0.

- **CSCtx68100**
  Symptoms: On a system having SP-RP, the reload reason is not displayed correctly. Once the system crashes, in all subsequent reloads the last reload reason is displayed as crash.
  Conditions: The symptom is observed on a system having SP-RP. The reload reason is shown wrongly when the `show version` CLI is executed.
  Workaround: There is no workaround.

- **CSCtx74342**
  Symptoms: After interface goes down or is OIRed, in a routing table you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next hop interface set to the interface that is down.
  Conditions: The symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).
  Workaround: Configuring SPF throttle timer can change the interval.
  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:
  ```
  Router show ipv6 route
  IPv6 Routing Table - default - 2 entries
  Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
           B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
          IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
  ```
Caveats

ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
l - LISP
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

O 2001::/64 [110/10]
   via Ethernet0/0, directly connected

• CSCtx86539
Symptoms: NAT breaks SIP communication with addition of media attributes.
Conditions: The symptom is observed with NAT of SIP packets.
Workaround: There is no workaround.

• CSCty03745
Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.
Conditions: This symptom occurs when the IPv4 default route exists, that is:
ip route 0.0.0.0 0.0.0.0 <next-hop>.
Or a certain static/IGP route exists: For example:
ip route 0.0.253.0 255.255.255.0 <next-hop>.
Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family.
For example:
router bgp 65000
    address-family l2vpn vpls
    neighbor 10.10.10.10 next-hop-self

Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

• CSCty05092
Symptoms: EIGRP advertises the connected route of an interface which is shut down.
Conditions: This symptom is observed under the following conditions:
1. Configure EIGRP on an interface.
2. Configure an IP address with a supernet mask on the above interface.
3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.
Workaround 1: Remove and add INTERFACE VLAN xx.
Workaround 2: Clear ip eigrp topology x.x.x.x/y.

• CSCty05150
Symptoms: After SSO, an ABR fails to generate summary LSAs (including a default route) into a stub area.
Conditions: This symptom occurs when the stub ABR is configured in a VRF without “capability vrf-lite” configured, generating either a summary or default route into the stub area. The issue will only be seen after a supervisor SSO.
Workaround: Remove and reconfigure “area x stub”.

- CSCty12083
  Symptoms: A Cisco 819 router with the C819HG+7 SKU reloads.
  Conditions: This symptom is observed on a Cisco 819 router with the C819HG+7 SKU reloads while running Cisco IOS Release 15.1(4)M3.8.
  Workaround: There is no workaround.

- CSCty32232
  Symptoms: BRI interface is not showing as monitored.
  Conditions: The issue occurs after performing an on-line insertion/removal of an NM-16ESW module.
  Workaround: Reload the router.

- CSCty32851
  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to “multilink ppp”.
  Conditions: The symptom is observed when the interface is configured with a VRF.
  Workaround: Shut down the interface before making the encap configuration change.

- CSCty41067
  Symptoms: Router crashes while doing an SSO without any configurations.
  Conditions: The symptom is observed while doing an SSO.
  Workaround: There is no workaround.

- CSCty54434
  Symptoms: ISRG2 with ISM VPN is not bringing up more than one tunnel in a crypto map-based scenario. This can happen with either certificates or PSK.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T and Cisco IOS Release 15.2(2)T.
  Workaround: Configure IKEv2 fragmentation so that the fragmentation/reassembly is handled by IKE code rather than by IPsec.

- CSCty54718
  Symptoms: A Cisco 3945 router crashes with configuration greater than 40k DN numbers of SAF/EIGRP.
  Conditions: This symptom is seen with the reset of CUCM several times. The router crashes, and a memory leak is seen.
  Workaround: There is no workaround.

- CSCty65189
  Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.
  Conditions: The symptom is observed when ZBFW is configured.
  Workaround: There is no workaround.

- CSCty65334
  Symptoms: Unconfigured crypto ACL causes the Cisco 3900 router to crash.
Caveats for Cisco IOS Release 15.2(1)T

Caveats

Conditions: This symptom is observed with a Cisco 3900 image with ISM crypto engine installed and enabled. This may also affect the Cisco 2900 and Cisco 1900 routers with ISM crypto engine installed and enabled.

Workaround: When changing the crypto ACL configuration, disable the ISM crypto engine first using the `no crypto engine slot 0` command, and then change the ACL. After changing the ACL, reload the router with ISM enabled.

- **CSCty77190**
  Symptoms: DTLS is switched back to TLS after reconnect.
  Conditions: This symptom is observed with the following conditions:
  - Test image c3845-advsecurityk9-mz.152-2.T1.InternalUseOnly
  - Test version - Cisco IOS Release 15.2(1)T
  Workaround: Restart the AnyConnect client.

- **CSCty78435**
  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.
  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.
  Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- **CSCty80553**
  Symptoms: Multicast router crashes.
  Conditions: The symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.
  Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- **CSCty86039**
  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.
  Conditions: This symptom is seen with tunnel interface with QoS policy installed.
  Workaround: There is no workaround.

- **CSCty94289**
  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.
  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.
  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- **CSCty96052**
  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.
Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.
Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty97961
   Symptoms: Device configured with SSLVPN crashes.
   Conditions: Device configured with SSLVPN and **functions svc-enabled** or **functions svc-required** and **svc dtls** and has an outbound ACL on one of the devices interface.
   This vulnerability has only been observed when the outbound ACL is tied to either a NAT or ZBFW interface in the outbound direction and is not the interface that the SSLVPN session is terminated against.
   This vulnerability has only been observed when the SSLVPN sessions terminate over PPP over ATM interface.
   This vulnerability was not able to be reproduced over SSLVPN sessions terminating over Ethernet or Serial interfaces.
   Workaround: Remove outbound ACL, or **no svc dtls** if running Cisco IOS Software that has a fix for Cisco bug ID CSCte41827.
   Further Problem Description: This bug covers configurations that have DTLS enabled on the device.
   A corresponding Cisco Bug ID CSCte41827, deals with a similar vulnerability but when the device does not have DTLS configured.
   PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:
   CVE ID CVE-2012-3924 has been assigned to document this issue.
   Additional information on Cisco’s security vulnerability policy can be found at the following URL:

- CSCty98834
   Symptoms: The Cisco c2900, c3900, and c1900 IOS with the ISM VPN crypto engine might crash after some time when you run out of memory on the ISM VPN engine as there are memory leaks during rekey.
   Conditions: This symptom occurs when the ISM VPN crypto engine is enabled.
   Workaround: Disable the ISM VPN module using the **no crypto engine slot 0** command.

- CSCty99846
   Symptoms: Cisco IOS Software includes a version of OpenSSL that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:
   CVE-2009-1386
   This bug was opened to address the potential impact on this product.
   Conditions: This symptom is observed on a device that is configured with SSLVPN and **svc dtls**.
   Workaround: Disable DTLS with **no svc dtls**.
   Further Problem Description: This problem would only be seen in Cisco IOS when using Anyconnect client with Cisco IOS SSLVPNs, after the initial session has been authenticated and established. Exploitation would result in Cisco IOS reloading.
PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:
CVE ID CVE-2009-1386 has been assigned to document this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:

- CSCtz13465
  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.
  Conditions: This symptom is observed with an interface with a policy installed.
  Workaround: There is no workaround.

- CSCtz13818
  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.
  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.
  Workaround 1: Refresh the updated route-target to use **clear ip route vrf vrf-name net mask**.
  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz25364
  Symptoms: GM to GM communication between ISM VPN and the Cisco ASR 1000 series router with TBAR enabled is broken.
  Conditions: This symptom occurs when ISM VPN and the Cisco ASR 1000 series router are GMs and TBAR is enabled.
  Workaround: Disable ISM VPN or disable TBAR and switch to counter-based anti-replay.

- CSCtz26735
  Symptoms: SDP process to provision CVO router is broken in Cisco IOS Release 15.2(3)T.
  Conditions: This symptom is seen when we start the SDP process. The connection immediately breaks after the username and password are entered.
  Workaround: There is no workaround.

- CSCtz27137
  Symptoms: An upgrade to the S639 or later signature package may cause a Cisco IOS router to crash.
  Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:
  - Cisco IOS Release 12.4(24)T4
  - Cisco IOS Release 15.0(1)M4
  - Cisco IOS Release 15.0(1)M8
  - Cisco IOS Release 15.2(3)T
  Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:
- Access the router via the console.
- Enter break sequence to access ROMmon mode.
- Change the config-register value to 0x2412.
- Boot the router to bypass the startup-configuration.
- Configure the basic IP parameters.
- TFTP a modified configuration to the router’s running-configuration with Cisco IOS IPS disabled.
- Reset the config-register to 0x2102.
- Enter the `write memory` command and reload.

- **CSCtz44989**
  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.
  Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.
  Workaround: There is no workaround.

- **CSCtz51773**
  Symptoms: High CPU seen on routers equipped with an ISM-VPN module. The output of `show process cpu` shows that the process “REVT Background” is using around 70% of the CPU cycles.
  The ISM-VPN module is not visible in `show diag`, and the output of `show crypto engine configuration` indicates that the module status is DEAD.
  Conditions: The symptom is observed with an ISM VPN with a few IPSec tunnels. This can take between a day and a week.
  Workaround 1: Reload the router.
  Workaround 2: For a longer-run workaround and if the traffic volume is not too high, switch to the onboard crypto hardware using the configuration `no crypto engine slot 0`.

- **CSCtz58719**
  Symptoms: Watchdog timeout under interrupt or process
  Conditions: The symptom is observed with a QoS configuration applied. The issue happens because of resource contention between a process path packet and an interrupt path packet
  Workaround: Disable QoS

- **CSCtz70938**
  Symptoms: When the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.
  Conditions: This symptom occurs when the router is booted using boot commands and boot configuration other than startup-configuration (for example, a file on flash) and there are “service-module” CLI in the configuration, the router crashes.
  Workaround: Do not use boot configuration files other than startup-configuration when there are “service-module” CLI in the configuration.
Caveats

- **CSCtz80643**
  Symptoms: A PPPoE client’s host address is installed in the LNS’s VRF routing table with the `ip vrf receive vrf name` command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.
  Conditions: This symptom is observed only when the Virtual-access interface is configured with the `ip vrf receive vrf name` command via the Virtual-Template or RADIUS profile.
  Workaround: There is no workaround.

- **CSCua06598**
  Symptoms: Router may crash with breakpoint exception.
  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.
  Workaround: Disable SNMP IPv6 polling.

- **CSCua39107**
  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.
  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.
  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- **CSCua43930**
  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.
  Conditions: The issue is seen on a Cisco ISR G2.
  Workaround: There is no workaround.

- **CSCua47570**
  Symptoms: The `show ospfv3 event` command can crash the router.
  Conditions: The symptom is observed when “ipv4 address family” is configured and redistribution into OSPFv3 from other routing protocols is configured.
  Workaround: Do not use the `show ospfv3 event` command.

- **CSCua67998**
  Symptoms: System crashes.
  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.
  Workaround: There is no workaround.

- **CSCub17794**
  Symptoms: Cisco 819G routers with HSPA+ modems (8705 modems) will crash on bootup.
  Conditions: This symptom is observed in Cisco IOS interim Release 15.2(1)T2.8.
  Workaround: There is no workaround.
Resolved Caveats—Cisco IOS Release 15.2(1)T2

Cisco IOS Release 15.2(1)T2 is a rebuild release for Cisco IOS Release 15.2(1)T. The caveats in this section are resolved in Cisco IOS Release 15.2(1)T2 but may be open in previous Cisco IOS releases.

- **CSCtc96631**
  Symptoms: Packet drops occur in downstream devices every 4ms burst from shaper.
  Conditions: The symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.
  Workaround: Use ASRs instead of ISR.

- **CSTctj30238**
  Symptoms: WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there are no traffic matches in the class.
  Conditions: This issue is seen on the Cisco 7600 router with ES+ line card only. The Es+ line card does not support per WRED class based counters. There was a recent breakage due to the Transmit packets/bytes column that started showing up for the Es+ line card. This is wrong. As ES+ writes same value to WRED transmit count (not the per subclass base count, but total count), this value does not make sense.
  Workaround: Do not use WRED subclass Transmit packets/bytes counters for ES+ line card on the Cisco 7600 router.

- **CSCtk00181**
  Symptoms: Password aging with crypto configuration fails.
  Conditions: The symptom is observed when Windows AD is set with “Password expires on next log on” and the VPN client is initiating a call to NAS. NAS does not prompt for a new password and instead gives an Auth failure.
  Workaround: There is no workaround.

- **CSCtl04112**
  Symptoms: Switch/router reloads whenever NAS receives a state attribute in a COA request.
  Conditions: While parsing a COA request, a state attribute is decoded twice and the original pointer is moved ahead so that the next attribute type and length are wrong. This causes a loop which never exits.
  Workaround: Ensure state attribute is not received in a COA request.

- **CSCtl52854**
  Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.
  Conditions: The symptom is observed when a multicast server is connected to an EHWIC L2 interface.
  Workaround: Connect the multicast server to an on-board gig interface.

- **CSTcto63268**
  Symptoms: A Cisco 3900e router may crash while configuring a PRI-group on a VWIC2 in a native HWIC slot.
Conditions: The router must be a Cisco 3900e and the number of timeslots in the new PRI-group must be greater than the number of available DSPs. Additionally, a EVM-HD-8FXS/DID must be installed and the onboard DSPs must be configured for DSP sharing.

Workaroud: Remove the EVM or disable DSP sharing.

- CSCto71671

Symptoms: Using the `radius-server source-ports extended` command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

Workaroud: There is no workaround.

- CSCto89536

Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

Workarounds that mitigate these vulnerabilities are not available.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

- CSCto90912

Symptoms: A crash is seen with the DHCPv6 client process.

Conditions: The symptom is observed when `ipv6 address dhcp` is run on an “auto-template” interface, and then the interface is removed with a `no int auto-temp`.

Workaroud: There is no workaround.

- CSCto99343

Symptoms: Linecards do not forward packets which causes a failure on the neighborship.

Conditions: The symptom is observed on VSL-enabled linecards on a VSS system.

Workaroud: There is no workaround.

- CSCtq17082

Symptoms: Router reloads.

Conditions: The symptom is observed with at least 2000 IPSec tunnel sessions by automatic script to remove a QoS configuration from Virtual Template.

Workaroud: Session teardown before you remove the QoS configuration.

- CSCtq21234

Symptoms: Label is not freed.

Conditions: The symptom is observed after shutting down the link.

Workaroud: There is no workaround.
• CSCtq21258
  Symptoms: When a user uses a password larger than 32 bytes in size, the authentication for COA will pass if the password matches the settings on the RADIUS server. When this password is reduced in size to exactly 32 bytes, including the setting on the RADIUS server, the authentication for the COA will fail as the ISG appends excess data to the password sent to the RADIUS for authentication.
  Conditions: This symptom is seen when the user password is larger then 32 bytes and is being reduced to exactly 32 bytes.
  Workaround: Do not use 32 bytes as the size for the user password. In case the error occurs, the only method to solve the issue is to reload the device.

• CSCtq32282
  Symptoms: Chunk leaks observed on various platforms.
  Conditions: The issue seen while testing the ipsec_unify_solaris functionality.
  Workaround: There is no workaround.

• CSCtq36153
  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:
  – Memory Leak Associated with Crafted IP Packets
  – Memory Leak in HTTP Inspection
  – Memory Leak in H.323 Inspection
  – Memory Leak in SIP Inspection
  Workarounds that mitigate these vulnerabilities are not available.
  Cisco has released free software updates that address these vulnerabilities.
  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

• CSCtq61128
  Symptom: Router is crashing with Segmentation fault(11).
  Conditions: It was observed on routers acting as IPSEC hub using certificates.
  Workaround: There is no workaround.
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2011-4231 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

• CSCtq64987
  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.

Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

- **CSCtq68778**
  
  **Symptoms:** After an ISSU, the reload reason string is missing in the newly-active session.
  
  **Conditions:** The symptom is observed after an ISSU.
  
  **Workaround:** There is no workaround.

- **CSCtq78217**
  
  **Symptoms:** A router crashes with the following information:

  System returned to ROM by address error at PC 0xZZZZZZZZ, address 0xZZZZZZZZ
  
  **Conditions:** The symptom is observed with CUBE + SIP.
  
  **Workaround:** There is no workaround.

- **CSCtq86515**
  
  **Symptoms:** UDP Jitter does not detect packet loss on Cisco IOS Release 15.1.
  
  **Conditions:** This symptom occurs when traffic is dropped on the device sending the UDP Jitter probe. However, when traffic is dropped on another device, packet loss is detected.
  
  **Workaround:** Do not drop traffic on the device sending the UDP Jitter probe.

- **CSCtr01750**
  
  **Symptoms:** The command `clear ip nat translation *` is not working as expected.
  
  **Conditions:** Issue is seen with a Cisco 7200 platform that is running the Cisco 15.2 (0.19)T0.1 image. This issue is specific to the NAT translations created for ICMP traffic sent with port number 0.
  
  **Workaround:** There is no workaround.

- **CSCtr04829**
  
  **Symptoms:** A device configured with “ip helper-address” drops packets because of a zero hardware address check.
  
  **Conditions:** This symptom occurs when the hardware address is zero.
  
  **Workaround:** There is no workaround.

- **CSCtr11469**
  
  **Symptoms:** CNS configurations might crash the HA system, especially on the standby side.
  
  **Conditions:** The symptom is observed when CNS features run on any HA system.
  
  **Workaround:** Do not use CNS features on HA system.

- **CSCtr14675**
  
  **Symptoms:** The line card crashes after removing the child policy in traffic.
  
  **Conditions:** This symptom occurs after the child policy is removed in traffic.
  
  **Workaround:** There is no workaround.
Caveats for Cisco IOS Release 15.2(1)T

- **CSCtr20762**
  Symptoms: L3VPN tunnel is not coming up after the router is reloaded.
  Conditions: The symptom is observed with “aaa system accounting” configured and when the TACACS server is not reachable.
  Workaround 1: Disable “aaa system accounting”.
  Workaround 2: Ensure the TACACS server is reachable.

- **CSCtr25386**
  Symptoms: BFDv6 static route association fails after reenabling interfaces.
  Conditions: This symptom is observed after interfaces are reenabled.
  Workaround: There is no workaround.

- **CSCtr31496**
  Symptoms: The line card crashes after switchover with the multilink configurations.
  Conditions: This symptom occurs after switchover with the multilink configurations.
  Workaround: There is no workaround.

- **CSCtr33856**
  Symptoms: Traceback and/or watchdog crash, with decodes pointing to mace_monitor_waas_command@.
  Conditions: The symptom is observed with on the fly changes to mace policies and classes.
  Workaround: There is no workaround.

- **CSCtr35740**
  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.
  Conditions: The symptom is observed when the DMVPN tunnel active link goes down.
  Workaround: There is no workaround.

- **CSCtr45978**
  Symptoms: Cisco IOS WAAS has FTP or HTTP connections hung in CONN_ABORT state.
  Conditions: Device configured with Cisco IOS WAAS, and crafted FTP packets or real HTTP user traffic to internet sites is passed across the WAN link.
  Has only been observed on 15.2(1)T IOS Code.
  Once the connection limit is reached and the rest of the connections started going pass-through.
  Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.1:
No CVE ID has been assigned to this issue.
Caveats for Cisco IOS Release 15.2(1)T

Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCtr49064**

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

  The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

- **CSCtr51786**

  Symptoms: The command `passive-interface` for a VNET auto-created subinterface x/y.z may remove the derived interface configuration command `ip ospf process id area number`. Consequently, putting back `no passive-interface` command will not form the lost OSPF ADJ.

  Conditions: The symptom is observed only with interfaces associated with the OSPF process using the command `ip ospf vnet area number`.

  Workaround: Associate the interface with the OSPF process using a network statement or using the interface command `ip ospf process id area number`.

  Further Problem Description: Interfaces associated with a process using a network statement under “router ospf” or interfaces configured with the command `ip ospf process id area number` are not affected.

- **CSCtr52740**

  Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.

  Conditions: The symptom is observed when querying history information from `rttMonHistoryCollectionCompletionTime` object using invalid indices.

  Workaround: Instead of using “get”, use “getnext” to list valid indices for the MIB OID.

- **CSCtr66487**

  Symptoms: Packet drops beyond 1492 MTU size with MPLS L2VPN Xconnect configuration.

  Conditions: The symptom is observed when you ping mpls pseudowire 10.0.0.1 101 size 1493 and above.

  Workaround: There is no workaround.

- **CSCtr79347**

  Symptoms: A Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
  Traceback summary
  % 0x80e7b6 : __be_bgp_tx_walker_process
  % 0x80e3bc : __be_bgp_tx_generate_updates_task
  % 0x7f8891 : __be_bgp_task_scheduler
Conditions: No conditions but this is a rarely observed issue.
Workaround: There is no workaround.

- CSCtr79905
  Symptoms: Error message seen while detaching and reattaching a service policy on an EVC interface.
  Conditions: The symptom is observed when detaching and reattaching the service policy on an EVC interface when port shaper is configured on the interface.
  Workaround: There is no workaround.

- CSCtr81559
  Symptoms: The PPP session fails to come up occasionally on LNS due to a matching magic number.
  Conditions: This symptom is observed during LCP negotiation, when the random magic number generated on the client matches the magic number generated on the LNS. PPP assumes it to be a loopback and disconnects the PPP session. This condition occurs rarely.
  Workaround: To avoid this, renegotiate the LCP. Configure the client using the `retry` command. This may cause the next session to come up correctly.

- CSCtr87740
  Symptoms: A router may crash due to a bus error.
  Conditions: The symptom seems to be related to high traffic and an ongoing rekey taking place.
  Workaround: There is no workaround.

- CSCtr92779
  Symptoms: Call scenario is with Avaya CM6 over TLS/SIP trunks which causes the Cisco 3945 router (running Cisco IOS Release 15.1(4)M1) CUBE to crash.
  Conditions: The symptom is observed when a call is originated from Cisco Phone A via TLS/SIP Trunk to CUBE (3945 15.1(4)M1), to Avaya CM6 Phone A which is set to “call forward all” back to the original Cisco Phone A.
  Workaround: There is no workaround.

- CSCtr97640
  Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.
  Conditions: None.
  Workaround: None--Physically securing the router is important.


- CSCts11344
  Symptoms: Upon a reload, a router will crash during bootup.
  Conditions: The symptom is observed on a Cisco 3900 series router with “no cry eng slot 0” configured then the configuration is saved in the startup config file. The issue is seen upon a reload.
Workaround: Do not save “no cry eng slot 0” in the config file. If you want to turn off the crypto engine, do it after router boot up.

Further Problem Information: To recover from the crash, first reload an image build before 07/07/2011. Remove “no cry eng slot 0” from the startup configuration then reload the image you are going to use. After the router boots up, configure “cry eng slot 0” to turn off the engine.

- CSCts11594
  Symptoms: A mediatrace session is scheduled with an attached session-parameter. The session is unscheduled and the session-parameters removed so that the default session parameters should be used.
  On the first schedule, traceback is seen. The session is again unscheduled and scheduled for second time and a crash is seen.
  Conditions: The symptom is observed when using custom session-parameters for a session and then removing it. Then using the default session-parameters followed by scheduled and unscheduled twice.
  Workaround: Use either the default session-parameters or custom session-parameters. Do not toggle between both.

- CSCts27042
  Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.
  Conditions: The symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).
  Workaround: There is no workaround.

- CSCts28315
  Symptoms: A DHCP PD request does not accept a specific server.
  Conditions: The symptom is observed because the router does not include any IA Prefix option in Request message. This is correct behavior of RFC:
  http://tools.ietf.org/html/rfc3633#section-10
  A requesting router may set the IPv6 prefix field to zero and a given value in the prefix-length field to indicate a preference for the size of the prefix to be delegated.
  Workaround: There is no workaround.

- CSCts38291
  Symptoms: When configuring 6VPE you may see prefix corruption. Advertised prefix is different than the one installed. RD value also changes as well.
  Conditions: The symptom is observed when configuring “vpn6 address family”.
  Workaround: There is no workaround.

- CSCts38429
  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.
  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

- CSCts38674
  Symptoms: UUT/modem fails to make a call using external dialer interface.
Caveats for Cisco IOS Release 15.2(1)T

Conditions: The symptom is observed when the cellular interface is configured with “no ip address” and when using an external dialer interface. UUT/modem will fail to make a call.

Workaround: Configure cellular interface with “ip address negotiated”.

- CSCts55371
  Symptoms: OSPF will not flood link state updates over an interface. The command `show ip ospf flood-list` will show interface entries similar to:

  Interface Tunnel1, Queue length 181
  Link state retransmission due in 1706165974 msec
  Note the high value for the retransmission timer.

  Conditions: The symptom is observed with some newer S and T releases including Cisco IOS Release 15.1(2)S, Release 15.1(3)S, and Release 15.2(1)T.

  The issue can occur on interfaces where OSPF has not flooded updates for more than 24 days. This can include interfaces that are newly configured for OSPF if the router has been up longer than that. Interfaces that flood LSAs at least once every 24 days will not be affected.

  Workaround: To clear a hung interface use `clear ip ospf process`.

- CSCts57108
  Symptoms: Standby reloads continuously after ISSU RV.

  Conditions: The symptom is observed during a downgrade scenario where the active is running Cisco IOS Release 15.1 and the standby is running Release 12.2. Cisco IOS Release 15.1 will be syncing “snmp-server enable traps ipslal” keyword to the standby, but the standby does not understand the new keyword.

  Workaround: Remove references to “snmp-server enable traps ipslal” and then perform the downgrade.

- CSCts62082
  Symptoms: Router generates the following message:

  `%NHRP-3-QOS_POLICY_APPLY_FAILED: Failed to apply QoS policy 10M-shape mapped to NHRP group xx on interface Tunnelxx, to tunnel x.x.x.x due to policy installation failure`

  Conditions: The symptom is observed when “per-tunnel” QoS is applied and there are more than nine DMVPN spokes. (Up to eight spokes, with QoS applied is fine.)

  Workaround: There is no workaround.

- CSCts63973
  Symptoms: Router configured with ScanSafe can crash with high session testing. This happens very rarely and is not seen frequently.

  Conditions: The symptom is observed when ScanSafe is configured and HTTP sessions are created at a high rate.

  Workaround: There is no workaround.

- CSCts64539
  Symptoms: The BGP next hop is inaccessible. The `show ip route` command output in the global and VRF routing tables shows that the next hop is reachable. The `show ip bgp vpnv4 all attr next-hop` command output shows max metric for the next hop.

  Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

  Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.
Caveats

Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

Workaround 3: If “neighbor x.x.x.x disable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- CSCets67423

Symptoms: On the Cisco ASR1k and ISR G2 only, call failures occur in the CUBE enterprise with interoperability to third-party SIP devices due to a trailing comma in the Server and User-Agent fields. For example:

User-Agent: Cisco-SIPGateway/IOS-15.1(3)S,
Server: Cisco-SIPGateway/IOS-15.1(3)S,

You might see this with Cisco IOS Release 15.2(1)T or other versions. If the trailing comma is present it can cause interoperability issues. If there is no trailing comma, then this defect is not applicable.

Conditions: This symptom is observed when there is an interoperability problem between the CUBE enterprise and a third-party SIP device. The trailing comma is invalid against RFC 2616 and the third-party SIP device ignores SIP messages from the CUBE.

Workaround: On both inbound and outbound dial peers, apply a SIP profile similar to the one below, or add the four lines to an existing SIP profile in use.

```
voice class sip-profile 1
  request ANY sip-header User-Agent modify "-15.*," ""
  response ANY sip-header User-Agent modify "-15.*," ""
  request ANY sip-header Server modify "-15.*," ""
  response ANY sip-header Server modify "-15.*," ""

dial-peer voice 1 voip
  voice-class sip profiles 1
```

- CSCets67465

Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

Conditions: The symptom is observed always, if the standby is configured as an SSO.

Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCets69204

Symptoms: PPPoE sessions do not get recreated on the standby RP.

Conditions: This symptom occurs on the standby RP.

Workaround: There is no workaround.

- CSCets85459

Symptoms: Upon a reload, the cellular interface will not negotiate if a crypto map is applied to it.

Conditions: The symptom is observed on a Cisco 881 router that has a cellular interface which dials to get an IP address and also acts as the VPN gateway. When we reload the router, the cellular interface does not connect if a crypto map is applied and we see IPsec fails to initialize because we do not have an IP address.

Workaround: This situation remains until we manually remove the crypto map from the cellular interface. Then we see the chat-script starting and the whole dialing procedure starts, then the cellular link is up with an IP address. Then we re-apply the crypto map again and the tunnel works fine.
- **CSCts88467**
  Symptoms: Drops happen earlier than expected.
  Conditions: This symptom occurs if the queue-limit is incorrectly calculated.
  Workaround: Configure a queue-limit explicitly to fix this issue, then remove and reapply the policy. Configuring queue-limit in parent policy automatically triggers calculation based on the parent queue-limit value on the child queue-limits based on bandwidth allocated to various classes.

- **CSCtt05316**
  Symptoms: Under `show content-scan sessions active`, the usergroup information is printed over and over.
  Conditions: The symptom is observed when the TCP SYN is retransmitted.
  Workaround: There is no workaround.

- **CSCtt05910**
  Symptoms: Router crashes.
  Conditions: The symptom is observed when running the `show sum` command. It is seen with the Cisco 3900e platform.
  Workaround: Do not use the `show sum` command.

- **CSCtt11210**
  Symptoms: Routers enrolled to hierarchical PKI on different subordinate CAs, may be unable to establish tunnels using IKEv1/IKEv2.
  The “debug crypto isakmp” debugs will show that the certificate-request payload contains the issuer-name of the subordinate CA certificate, not the subject-name as it would be expected.
  Conditions: The symptom is observed when the router does not have the Root CA certificate installed.
  Workaround: Install the Root CA certificate in a separate trustpoint on all involved routers.

- **CSCtt16051**
  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.
  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.
  This advisory is available at the following link:

- **CSCtt17762**
  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.
  Conditions: The symptom is observed on an IP PIM multicast network.
  Workaround: There is no workaround.

- **CSCtt17879**
  Symptoms: The `bgp network backdoor` command does not have any effect.
  Conditions: This symptom occurs:
- On 64-bit platform systems.
- When the network is learned after the backdoor has been configured.

Workaround: Unconfigure and reconfigure the network backdoor.

- **CSCtt19027**
  Symptoms: When ACL is applied to the serial interface or Gigabit interface, ping failure seen even though the permit statement is there.
  Conditions: The symptom is observed when ACL is configured on the serial interface or Gigabit interface.
  Workaround: Enable EPM by installing the security license.
  Further Problem Description: This is seen with those images where EPM is not supported and because of that an EPM call always gives a return value as “deny” due to registry call.

- **CSCtt20215**
  Symptoms: Controller goes down after reload.
  Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.
  Workaround: Unplug/plug the cable, or reset link from PBX side.

- **CSCtt28703**
  Symptoms: VPN client with RSA-SIG can access a profile where his CA trustpoint is not anchored.
  Conditions: Use of RSA-SIG.
  Workaround: Restrict access by using a certificate-map matching the right issuer.

- **CSCtt33158**
  Symptoms: If WRED is already present and the queue limit is configured in packets then WRED thresholds become 0.
  Conditions: Use the below mentioned config to repro the problem.

```plaintext
policy-map parent
  class class-default
    shape aver 2000
    service-policy child

policy-map child
  class class-default
    random-detect
    int g0/0/0
    service-policy out parent

policy-map child
  class class-default
    queue-limit 2000
```
  Workaround: Remove WRED and reattach it.
- **CSCt43843**
  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.
  Conditions: It is occurring with a Cisco 7200 platform loaded with the 15.2 (1.14)T0.1 image.
  Workaround: There is no workaround.

- **CSCt45381**
  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
  An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.
  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

- **CSCtu11677**
  Symptoms: A Cisco router may unexpectedly reload due to bus error or segV exception or generate a spurious error when the cSipStatsSuccessOkTable snmp object is polled.
  Conditions: This is seen on a voice gateway when the cSipStatsSuccessOkTable snmp object is polled.
  Workaround: Create an SNMP view and then block the oid for cSipStatsSuccessOkTable and then apply it to all SNMP communities on the device:
  ```
  snmp-server view blockmib iso include
  snmp-server view blockmib 1.3.6.1.4.1.9.9.152.1.2.2.5 exclude
  ```
  and then apply it to the community:
  ```
  snmp-server community <community> view blockmib ro
  ```

- **CSCtu16809**
  Symptoms: Deny entries in the KS ACL are not downloaded to the GM when the GM has an ISM VPN card.
  Conditions: The GM is using an ISM VPN card.
  Workaround: Use deny entries on a local ACL on the GM, or disable the ISM VPN.

- **CSCtu18786**
  Symptoms: Device may crash showing “VOIP” error messages. Decodes point to voice functions.
  Conditions: The symptom is observed when SIP is enabled on the device.
  Workaround: There is no workaround.

- **CSCtu21967**
  Symptoms: A router configured to be an IP voice gateway may crash.
  Conditions: The exact conditions for this crash are currently unknown.
  Workaround: There is no workaround.
• CSCtu24740
Symptoms: A Cisco ISR router may unexpectedly reload due to bus error or Segv Exception or experience a spurious access.
Conditions: The symptom is observed when NAT and dampening are configured on the same interface while the device is running Cisco IOS Release 15.2(1)T or a later release.
Workaround 1: Remove dampening from the configuration.
Workaround 2: Downgrade to Cisco IOS Release 15.1(4)M or earlier release.

• CSCtu29881
Symptoms: A router may crash while using double authentication for IPsec (ESP + AH) and certain types of traffic.
The following message is seen in the crashinfo file:
validblock_diagnose, code = 1
current memory block, bp = 0xZZZZZZZZZ, memorypool type is I/O
data check, ptr = 0xZZZZZZZZZ
next memory block, bp = 0xZZZZZZZZZ, memorypool type is I/O
data check, ptr = 0xZZZZZZZZZ
previous memory block, bp = 0xZZZZZZZZZ, memorypool type is I/O
data check, ptr = 0xZZZZZZZZZ
The router crashes due to I/O memory corruption - block overrun.
Conditions: The symptom is observed with double authentication (AH + ESP) and certain type of packets.
Workaround 1: Do not using double authentication (AH + ESP). Use ESP instead.
Workaround 2: Use an IOS version that does not have the fix for CSCtc40806.

• CSCtu33956
Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.
Conditions: This symptom is observed under the following conditions:
– The PPPoE dialer client needs to be configured on the physical SHDSL interface.
– The GRE tunnel destination interface should point to the dialer interface.
– The MPLS pseudowire should go over the tunnel interface.
– After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.
Workaround: There is no workaround.

• CSCtu38244
Symptoms: After bootup, the GM cannot register and is stuck in “registering” state. Issuing the clear crypto gdoi command is required for a successful registration to the keyserver.
Conditions: The symptom is observed upon router bootup.
Workaround: Do a clear crypto gdoi after a reload.
Caveats

- **CSCtu52820**
  Symptoms: A memory leak is observed under HTTP PROXY Server process.
  Conditions: Device is configured with Cisco ISR Web Security with Cisco ScanSafe and has User Authentication NTLM configured.
  Workaround: There is no workaround.
  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C
  CVE ID: CVE-2011-4661 has been assigned to document this issue.
  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- **CSCtu57226**
  Cisco IOS Software contains a denial of service (DoS) vulnerability in the Wide Area Application Services (WAAS) Express feature that could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload.
  Cisco IOS Software also contains a DoS vulnerability in the Measurement, Aggregation, and Correlation Engine (MACE) feature that could allow an unauthenticated, remote attacker to cause the router to reload.
  An attacker could exploit these vulnerabilities by sending transit traffic through a router configured with WAAS Express or MACE. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to cause the router to leak memory or to reload. Repeated exploits could allow a sustained DoS condition.
  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-mace

- **CSCtv52031**
  Symptoms: Router crashes while accessing the usergroup database.
  Conditions: The symptom is observed with performance testing.
  Workaround: There is no workaround.

- **CSCtw50141**
  Symptoms: Incremental leaks at __be_ber_get_stringa pointing to LDAP process.
  Conditions: The symptom is observed when NTLM authentication is being used with an LDAP server and with the router acting as the NTLM proxy.
  Workaround: There is no workaround.

- **CSCtw56439**
  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.
  Conditions: The symptom is observed with IPsec and the **ip mtu** over a tunnel interface.
  Workaround: There is no workaround.

- **CSCtw60333**
  Symptoms: HTTP process hangs. This impacts the webauth authentication scaling factor.
Caveats for Cisco IOS Release 15.2(1)T

CSCtw71620
Symptoms: ISM VPN module cannot handle SSL records of a size greater than 1500 bytes. It will lead to SSL record encrypt/decrypt operation failure and result in a packet drop.
Conditions: The symptom is observed with ISM VPN and SSL records of a size greater than 1500 bytes.
Workaround: Disable the ISM VPN module with **no crypto engine slot 0**.

CSCtw76044
Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.
Conditions: The symptom is observed under all conditions.
Workaround: There is no workaround.

CSCtw99290
Symptoms: The source or destination group-address gets replaced by another valid group-address.
Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.
Workaround: There is no workaround.

CSCtx06018
Symptoms: Interface queue wedge is seen when performing WAAS performance test.
Conditions: The symptom is observed when performing WAAS performance test.
Workaround: Increase interface input queue hold size.

CSCtx06801
Symptoms: Certain websites may not load when content-scan is enabled. Delays of up to a few seconds may be seen.
Conditions: The symptom is observed when content-scan is enabled.
Workaround: Though not always, refreshing the page sometimes helps.
Further Problem Description: The problem is due to GET request being segmented. For example, a huge get request of 1550 may come from the client in two different packets such as 1460+90=1550.

CSCtx12216
Symptoms: I/O pool memory goes low.
Conditions: The symptom is observed with Scansafe configured. A small buffer is not getting freed.
Workaround: There is no workaround.
• **CSCtx16040**
  Symptoms: ISM VPN card will crash when used in combination with SSL-AO of WAAS express. In theory, this can also happen in normal VPN-SSL.
  Conditions: The symptom is observed with high numbers of SSL connections.
  Workaround: Disable the ISM VPN card.

• **CSCtx37680**
  Symptoms: All the ports on the ISR are used up. After this we may see a crash.
  Conditions: The symptom is observed with ports on the ISR.
  Workaround: Ensure that not all the TCP ports on the ISR are allocated.

• **CSCtx46741**
  Symptoms: ISM VPN module crashes for SSL records between 1800 bytes to 1840 bytes.
  Conditions: The symptom is observed with an ISM VPN module + SSLVPN or ISM VPN + WAAS SSL AO.
  Workaround: Disable ISM VPN module and fallback to onboard/SW crypto engine.

• **CSCtx47493**
  Symptoms: NTLM authentication does not work.
  Conditions: The symptom is observed when “ip admission ntlm rule” is configured on the interface.
  Workaround: There is no workaround.

**Resolved Caveats—Cisco IOS Release 15.2(1)T1**

Cisco IOS Release 15.2(1)T1 is a rebuild release for Cisco IOS Release 15.2(1)T1. The caveats in this section are resolved in Cisco IOS Release 15.2(1)T1 but may be open in previous Cisco IOS releases.

• **CSCsh39289**
  Symptoms: A router may crash under a certain specific set of events.
  Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.
  Workaround: There is no obvious workaround, but the problem is unlikely to occur.

• **CSCtd15853**
  Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.
  Conditions:
  - mVPN is configured on the PE router.
  - Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.
  
  *Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier*
  
  
  Workaround: There is no workaround.
• CSCth11006
  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of
  service (DoS) vulnerabilities in the translation of the following protocols:
  – Session Initiation Protocol (Multiple vulnerabilities)
  – H.323 protocol
  All the vulnerabilities described in this document are caused by packets in transit on the affected
  devices when those packets require application layer translation.
  Cisco has released free software updates that address these vulnerabilities.
  This advisory is posted at

• CSCti33159
  Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed
  to using the directly-connected link.
  Conditions: This is seen when the border has multiple internal interfaces and one of the internal
  interfaces is directly connected to a neighbor and the other interface is one hop away.
  Workaround: There is no workaround.

• CSCtj47822
  Symptoms: The standby RP is stuck in standby_issu_negotiation_late state after a switchover and
does not come to SSO. Also, memory leaks are seen at tid_cmn_add_or_find_port_info.
  Conditions: The issue occurs during the peer (standby RP) reset or switch-over.
  Workaround: There is no workaround.

• CSCtj56551
  Symptoms: The Cisco 7600 crashes in a very rare case.
  Conditions: This symptom is observed very rarely when route-churn/sessions come up.
  Workaround: There is no workaround.

• CSCtk69114
  Symptoms: RP resets while doing ESP reload with crypto configuration.
  Conditions: This symptom is observed by unconfiguring and configuring interface configuration and
  reloading both ESPs. The RP crashes on the server.
  Workaround: There is no workaround.

• CSCtl50815
  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently
  without any actual routing changes:
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  Conditions: The symptom is observed under the following conditions:
  – Use ECMP.
  – Use mode monitor passive.
Caveats for Cisco IOS Release 15.2(1)T

Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtn21501
  Symptoms: A Cisco 2900 series router with switch modules (such as HWIC-4ESW-POE or HWIC-D-9ESW-POE) does not respond to SNMP queries on the BRIDGE-MIB.
  Conditions: The symptom is observed on a Cisco 2900 series router (with switch modules) that is running Cisco IOS Release 15.x.
  Workaround: There is no workaround.
  Further Problem Description: This issue is similar to CSCsb46470.

- CSCtn39950
  Symptoms: An IPsec session will not come up.
  Conditions: This symptom occurs if a Cisco ISR G2 has an ISM VPN accelerator and slow interfaces such as BRI-PRI. Crypto plus ISM VPN module plus slow interfaces will not work.
  Workaround: Disable the ISM VPN module and switch to the onboard crypto engine.

- CSCtn58128
  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.
  Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.
  Workaround: Ensure that “no logging console” is configured.

- CSCtn62287
  Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.
  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.
  Workaround: There is no workaround.

- CSCto08135
  Symptoms: When a deny statement is added as the first ACL, the message gets dropped.
  Conditions: An ACL with deny as the first entry causes traffic to get encrypted and denied.
  Workaround: Turn off the VSA, and go back to software encryption.

- CSCto81701
  Symptoms: The PfR MC and BR sessions flap.
  Conditions: The symptom is observed with a scale of more than 800 learned TCs.
  Workaround: Use the following configuration:

    \[ \text{pfr master keepalive 1000} \]
- **CSCto88393**
  Symptoms: CPU hogs are observed on a master controller:
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0), process = OER Master Controller.
  Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.
  Workaround: There is no workaround.

- **CSCto99343**
  Symptoms: Linecards do not forward packets which causes a failure on the neighborship.
  Conditions: The symptom is observed on VSL-enabled linecards on a VSS system.
  Workaround: There is no workaround.

- **CSCtq29554**
  Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the `show ipc port | in MRIB` command on a failed line card does not display a port.
  Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.
  Workaround: Reload the failing line card to recover it.

- **CSCtq31898**
  Symptoms: Web traffic is not getting redirected to ScanSafe towers.
  Conditions: Having dual WAN links to reach the ScanSafe tower and the source interface used as a loopback.
  Workaround: There is no workaround.

- **CSCtq56727**
  Symptoms: Bulk call failures occur during heavy traffic loads, followed by a gateway crash.
  The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP, and other processes.
  “show proc mem sorted” shows a continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway is constant.
  Conditions: This symptom occurs when the SIP trunk in Unified Communications Manager pointing to the gateway is configured with a DTMF signaling type of “no preference” and the SIP gateway is configured with DTMF relay as sip-kpml.
  Workaround: There are two workarounds:
  1. Set the DTMF signaling type as “OOB and RFC 2833” in the Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
  2. Configure “dtmf-relay rtp-nte” (instead of “sip-kpml”) in the SIP gateway dial-peer configuration. The Unified Communications Manager is configured with “no preference.”
  Recovery: In order to recover from the crash, you must reload the gateway router.

- **CSCtq58383**
  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.
Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq62759
  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.
  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.
  Workaround: Use the `clear clns route` command or the `clear isis *` command.

- CSCtq71344
  Symptoms: Sometimes HTTPS sessions may fail when they are redirected via a ScanSafe tower.
  Conditions: This symptom is observed when multiple HTTPS sessions are being redirected to ScanSafe towers by the content-scan feature.
  Workaround: White-list the HTTPS traffic not to be redirected to ScanSafe towers by applying an ACL in the content-scan configuration.

- CSCtq75008
  Symptoms: A Cisco 7206 VXR crashes due to memory corruption.
  Conditions:
  - The Cisco 7206 VXR works as a server for L2TP over IPsec.
  - Encryption is done using C7200-VSA.
  - More than two clients are connected.
  If client sessions are kept up for about a day, the router crashes.
  Workaround: There is no workaround.

- CSCtq80648
  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.
  For example:
  ```
  interface Ethernet1/0
  vrf forwarding vpn1
  ipv6 address 1::1/64
  
  router bgp 65000
  address-family ipv6 vrf vpn1
  neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
  
  If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.
  
  Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.
  
  Conditions: This symptom occurs when a user changes the VRF assignment.
Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- **CSCtq80858**
  Symptoms: A router crashes randomly at various decodes.
  Conditions: This symptom is observed when MACE and IP SLA TCP-based probes are configured.
  Workaround: There is no workaround.

- **CSCtq83468**
  Symptoms: 302 Page Moved to url: https://<virtual-ip>/login.html?redirect-url=<actual-url> does not happen, and the client is directly presented with the login page.
  Conditions: The Proxy Auth method and ip admission virtual-ip should be configured.
  Workaround: Unconfigure ip admission virtual-ip.

- **CSCtq90577**
  Symptoms: A router crashes when removing NetFlow.
  Conditions: The symptom is observed when removing NetFlow.
  Workaround: There is no workaround.

- **CSCtq92182**
  Symptoms: An eBGP session is not established.
  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.
  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- **CSCtq92940**
  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.
  Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.
  Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.
  Further Problem Description: Please see the original bug (CST19967) for more information.

- **CSCtq96329**
  Symptoms: Router fails to send withdraws for prefixes, when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.
  Conditions: This symptom can happen only when bgp deterministic-med is configured.

The following releases are impacted:
- Cisco IOS Release 15.0(1)S4
- Cisco IOS Release 15.1(2)T4
- Cisco IOS Release 15.1(3)S
- Cisco IOS Release 15.2(1)T
Workaround: Disable deterministic med in the network/AS by issuing the no bgp deterministic-med command and then the clear ip bgp * command or hardreset of BGP session to remove any stale prefixes.

It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtr09142
  Symptoms: Poor throughput is observed with content-scan.
  Conditions: This symptom occurs when content-scan is enabled.
  Workaround: There is no workaround.

- CSCtr10577
  Symptoms: The following error message may be seen:
  OCE-3-OCE_FWD_STATE_HANDLE limit reached.
  Conditions: This symptom is observed under high traffic.
  Workaround: There is no workaround.

- CSCtr11620
  Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.
  Conditions: This symptom is observed when a Cisco 2911 is used.
  Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr14763
  Symptoms: A BFD session is always up, although the link protocol is down.
  Conditions: First the BFD session is up between the routers. After the VLAN is changed on the switch between the routers, the BFD peer is not reachable but the BFD sessions are always up.
  Workaround: There is no workaround.

- CSCtr19922
  Symptoms: Lots of output printed by show adjacency [key of adj] internal dependents followed by a crash.
  Conditions: The symptom is observed with the existence of midchain adjacencies, which will be created by IP tunnels, MPLS TE tunnels, LISP, and similar tunneling technologies.
  Workaround: Do not use the show adjacency [key of adj] internal dependents command. Specifically, it is the “dependents” keyword which is the problem. If the dependents keyword is not used there is no problem.

- CSCtr25734
  Symptoms: A router crashes.
  Conditions: This symptom is observed when the router is reloaded with a BRI interface brought up in startup configuration.
  Workaround: There is no workaround.
• CSCtr28857
A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.
Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

• CSCtr34965
Symptoms: An SSL WebVPN page does not come up when ISM-VPN is used.
Conditions: When an attempt is made to bring up an SSL session with ISM-VPN, the page does not load.
Workaround: There is no workaround.

• CSCtr40091
Symptoms: A call is not recorded.
Conditions: This symptom is observed after a few days of load.
Workaround: There is no workaround.

• CSCtr45608
Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.
Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when “set vrf” is configured on the route-map and the VRF is IPv6 only.
Workaround: Configure “ipv4 vrf” along with “ipv6 vrf” and refer “ipv6 vrf” on the route-map by configuring “ipv6 policy” on the ingress interface.

• CSCtr45633
Symptoms: A BGP dynamic neighbor configured under VPNv4 address-family does not work correctly.
Conditions: The symptom is observed when a BGP dynamic neighbor is configured under a VPNv4 address-family.
Workaround: Add “dynamic neighbor peer-group” under “ipv4 unicast address-family”.

• CSCtr54269
Symptoms: CUBE sends an RTCP BYE message to MS OCS R2, causing loss of audio for about 20 seconds.
Conditions: CUBE sends an RTCP BYE message only upon reINVITE due to session refresh timer.
Workaround: Downgrade to Cisco IOS Release 12.4(22)YB.

• CSCtr54907
Symptoms: A router crashes.
Conditions: This symptom is observed when an ISM VPN accelerator is used as the crypto engine.
Workaround: Disable the ISM VPN accelerator.

• CSCtr59314
Symptoms: A router reloads when the clear crypto session command is issued with 4000 sessions up.
Caveats

Conditions: This symptom is observed only under load conditions.
Workaround: There is no workaround.

- CSCtr63462

Symptoms: A router crashes at bootup.
Conditions: This symptom is observed with a Cisco 3900 that has an ISM VPN module installed and no HSECK9 license installed.
Workaround: Boot with a pre-15.2(1)T image, load an HSECK9 license, and then boot with a 15.2(1)T image.

- CSCtr83542

Symptoms: When content-scan functionality is enabled, the throughput drastically comes down and CPU utilization approaches 100 percent.
Conditions: This symptom is observed when content-scan is enabled and web traffic is subjected to redirection.
Workaround: Disable content-scan functionality.

- CSCtr85537

Symptoms: The content-scan feature was not available in the v152_1_t throttle before this DDTS was committed.
Conditions: All ISRG2 images.
Workaround: There is no workaround.

- CSCtr87249

Symptoms: A Cisco 2900 router crashes while it is reloaded with a 15.2(1.6)T image.
Conditions: This symptom occurs when an ISM-VPN card is installed on the Cisco 2900 and when there is no HSECK9 license installed.
Workaround: When the HSECK9 license is installed on the Cisco 2900, the crash is not seen.

- CSCtr89322

Symptoms: NME-RVPN module is not recognized by a Cisco 3900e router.
Conditions: The symptom is observed with a Cisco 3900e router.
Workaround: There is no workaround.

- CSCtr89882

Symptoms: Platform-related error messages are seen during an LDP flap in an ECM scenario.
Conditions: This symptom is observed with LDP with ECMP paths and during flapping of LDP sessions.
Workaround: There is no workaround.

- CSCtr91106

A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

Products that are not running Cisco IOS Software are not vulnerable.
Cisco has released free software updates that address these vulnerabilities.
The HTTP server may be disabled as a workaround for the vulnerability described in this advisory. This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- **CSCtr91890**
  Symptoms: An RP crashes sometimes when the router is having PPPoX sessions.
  Conditions: If a PPPoX session is terminated in the middle of session establishment and ip local pool is configured to pick the IP address for the peer and the version that the router is running has the fix for CSCtr91890.
  Workaround: There is no known workaround.

- **CSCtr94887**
  Symptoms: Using MRCP v1, VXML script with ASR operation will always receive no input event.
  Conditions: The symptom is observed with Cisco IOS Release 15.2(1)T.
  Workaround: There is no workaround.

- **CSCts06776**
  Symptoms: Requests hang when NAT is enabled.
  Conditions: This symptom is observed when content scan and NAT are enabled.
  Workaround: There is no workaround.

- **CSCts16285**
  Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP timeout. In the worst case, the line card may become disconnected if timeouts continue for a long period.
  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.
  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- **CSCts28462**
  Symptoms: snmp-server host 1.2.3.4 traps version 2c public nhrp is reported as snmp-server host 1.2.3.4 traps version 2c public ds3.
  Conditions: Unknown.
  Workaround: There is no workaround.

- **CSCts33952**
  Symptoms: An rsh command fails from within TclScript. When rsh command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.
  Conditions: This symptom is observed in Cisco IOS releases after 12.4(15)T14.
  Workaround: There is no workaround.

- **CSCts39535**
  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.
Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts64483
  Symptoms: Incorrect packet lengths are received at ISM VPN.
  Conditions: Buffer alignment in Cisco IOS software.
  Workaround: There is no workaround.

---

Open Caveats—Cisco IOS Release 15.2(1)T

All the caveats listed in this section are open in Cisco IOS Release 15.2(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCso41274
  Symptoms: The router has enough DSP resources to set up 14 signaling channels. While trying to configure a ds0-group for 16 time-slot, an error message is received that not enough DSP resources are available.
  Immediately after that the router spits the following traceback or may crash.
  Example:
  ```
sip-cme(config)#controller t1 1/0
sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-imm
sip-cme(config-controller)#ds0-gr 1 time 1-16 type e&m-immediate-start
% Not enough DSP resources available to configure ds0-group 1 on controller T1 1/0
% The remaining dsp resources are enough for 14 time slots.
% For current codec complexity, 1 extra dsp(s) are required to create this voice port.
sip-cme(config-controller)#
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x40C62 7A8 reading 0x4
%ALIGN-3-TRACE: -Traceback= 0x40C627A8 0x40D6769C 0x40D7281C 0x40D72E74 0x4036B0E4 0x4036D4B4 0x414C78EC 0x414EB3FC
Workaround: Ensure there are more DSPs in the router than signaling channels.
```

- CSCta22221
  Symptoms: A frame-relay client triggers the reload of a standby router.
Conditions: This symptom occurs if many frame relay-related configurations are present.
Workaround: There is no workaround.

• CSCtb51244
Symptoms: Spurious memory access is seen when deleting a policy map.
Conditions: The symptom is observed on a Cisco 7200 series router running Cisco IOS interim Release 12.4(24.6)PI11u.
Workaround: There is no workaround.

• CSCth38565
Symptoms: A router crashes after traffic stops and the WE router is unconfigured. This problem is intermittent and very difficult to reproduce.
Conditions: This symptom is observed when the WE is configured for full optimization, traffic is passed, and then the WE router is unconfigured. The type of traffic being passed does not seem to affect the crash.
Workaround: There is no workaround.

• CSCti13493
Symptoms: A router crashes and the following traceback is seen:
```
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 47523D58. - Process= "DSMP", ip= 0, pde= 226, -Traceback=
TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x430853EC
```
Conditions: The symptom is observed with the DSMP process.
Workaround: There is no workaround.

• CSCti33159
Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border as opposed to using the directly connected link.
Conditions: This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor, whereas the other interface is one hop away.
Workaround: There is no workaround.

• CSCti85075
Symptoms: Customer running cat4500-ipbasek9-mz.122-31.SGA9.bin on a cat4500 has reported the following log messages whenever an snmpset is performed:
```
%SCHED-3-SEMLOCKED: SNMP ENGINE attempted to lock a semaphore, already locked by itself -Traceback= 10DB0624 10C9FCD0 10C76964 10C6A300 10C901D0 10626B80 1061E388
```
The traceback may vary.
Conditions: This symptom is observed if the snmp engine is shut down during the processing of an snmpset. Entering the command `no snmp-server` in config mode is one way that the snmp engine can be shut down. The likelihood of the snmp engine being shut down during the processing of an snmpset is very small.
This problem will affect other devices, not just the Cat4500.
Workaround: There is no workaround other than to reboot the device.

• CSCtj59117
Symptoms: The following error message is seen and the router freezes and crashes:
%SYS-2-BADSHARE: Bad refcount in retparticle
A reload is required to recover.

Conditions: This symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Release 12.4(15)T14.
Workaround: Remove CEF.

- CSCAj69620
  Symptoms: An IPIPGW memory-related crash (double free) occurs at ccsip_update_srtp_caps.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCtk33149
  Symptoms: A router crashes when making SIP trunk calls along with Cisco IOS Firewall.
  Conditions: This symptom is observed with the Cisco UBE and the Cisco IOS Firewall configured as co-located, and with the Cisco IOS Firewall doing SIP inspection.
  Workaround: There is no workaround.

- CSCtk35917
  A service policy bypass vulnerability exists in the Cisco Content Services Gateway - Second Generation (CSG2) which runs on the Cisco Service Application Module for IP (SAMI). This vulnerability could allow in certain configurations:
  - Customers to access sites that would normally match a billing policy to be accessed without being charged to the end customer.
  - Customers to access sites that would normally be denied based on configured restriction policies.
  Additionally, Cisco IOS Software release 12.4(24)MD1 on the CSG2 contains two vulnerabilities that can be exploited remotely, via an unauthenticated attacker resulting in a denial of service of traffic through the CSG2. Both these vulnerabilities require only a single content service to be active on the CSG2 and are exploited via crafted TCP packets. A three way hand-shake is not required to exploit either of these vulnerabilities.
  No workarounds that mitigate these vulnerabilities are available.
  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110126-csg2

- CSCtk76648
  Symptoms: An rpcdump operation takes more time with WEXP.
  Conditions: This symptom is observed when WEXP is configured and an rpcdump occurs.
  Workaround: There is no workaround.

- CSCtk98248
  Symptoms: The Fa8 line proto is down after the connected device is reloaded.
  Conditions: This symptom is observed on the following platforms:
  - A Cisco 892 running Cisco IOS Release 15.0(1)M3 or a previous version
  - A Cisco 892 (only Fa8 port and set to 10/full)
  - A Cisco 3750/Cisco 2960 running Cisco IOS releases other than Cisco IOS Release 12.2(37)SE
  Workaround:
- Fa8 set to 100/full or auto
- On the Cisco 892, upgrade to Cisco IOS Release 15.0(1)M4
- On the Cisco 3750/Cisco 2960, run Cisco IOS Release 12.2(37)SE

- **CSCtl20181**
  Symptoms: Incorrect behavior is seen in MPPC compression.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCtl55502**
  Symptoms: Any parser command with a pipe option used in an http URL is not working properly and is giving the help option instead of actual output.
  Conditions: This symptom is observed when a parser command is used with a pipe option in an http URL. For example, http://<ipadd>/level/15/exec/show/runn//i/http/CR will not give proper output.
  Workaround: When using the router through a browser, enter the command through the text field instead of including it in the URL.

- **CSCtl79666**
  Symptoms: A Cisco 1801 router configured with zone-based firewall causes Memory Leak.
  Conditions: The symptom is observed with zone-based firewall configured on a Cisco 1801 router with traffic.
  Workaround: There is no workaround.

- **CSCtl87463**
  Symptoms: The queue length becomes negative.
  Conditions: This symptom is observed when Cisco IOS-WAAS is configured on the interface.
  Workaround: There is no workaround.

- **CSCtn04277**
  Symptoms: Time-based WRED does not work.
  Conditions: This symptom is observed when time-based WRED is used.
  Workaround: There is no workaround.

- **CSCtn14074**
  Symptoms: Ingress traffic passes through an unauthorized switch port.
  Conditions: This symptom is observed on a Cisco ISR G2 platform with an EHWIC-ESG module, and with ingress traffic initiated from an unauthorized supplicant port. To hit the scenario, supplicant should be authenticated and have a successful traffic flow. After that, simulate an UNAUTHORIZED state of supplicant, but traffic flow should not be stopped. Now, perform shut/no shut on the interface or reload the router to see that the traffic is continuing to go.
  Workaround: There is no workaround. However, if traffic is stopped prior to the symptom occurring, it will not be seen.

- **CSCtn16855**
  Symptoms: A Cisco 7200, PA-A3 cannot ping across an ATM pvc.
  Conditions: This symptom is observed when a high traffic rate output policy is applied under the pvc.
Caveats

Workaround: Remove the policy.

- CSCtn17800
  Symptoms: Main ATM interface statistics cannot be obtained using SNMP. This symptom is not observed for ATM subinterfaces/PVCs configured under subinterfaces or any other type of interfaces on a Cisco 3900 device.
  Conditions: This symptom is observed on a Cisco 3900 series running Cisco IOS Release 15.1T1.
  Workaround: There is no workaround.

- CSCtn24305
  Symptoms: The software version in “call home” messages has a trailing comma for the released images, which is causing a backend processing failure when the software version is needed.
  Conditions: This symptom is observed with all “call home” messages on all released images.
  Workaround: The backend can check to remove this trailing comma if it is present.

- CSCtn28941
  Symptoms: The PVDM2-24DM connection sequence stops at the debug output of “CSM: (CSM_PROC_WAIT_FOR_CARRIER)<--CSM_EVENT_MODEM_SETUP”, and therefore it cannot establish the connection with the TA, though NM-30DM can.
  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)T.
  Workaround: There is no workaround.

- CSCtn65519
  Symptoms: After a call connects through an MGCP-controlled gateway and DTMF is issued for a phone system to route a call, DTMF digits are not interpreted correctly.
  Conditions: This symptom is observed on an MGCP-controlled gateway.
  Workaround: Use H323.

- CSCtn84572
  Symptoms: A Cisco 2801 running Cisco IOS Release 12.4(24)T4 has good performance, but when upgraded to Cisco IOS Release 15.1(3)T, the performance may degrade.
  Conditions: This symptom is observed on a Cisco 2801 on both Cisco IOS images without any features configured.
  Workaround: There is no workaround.

  Further Problem Description: Without any features configured, both Cisco IOS versions tested the same (no performance decrease vs. each other). Then we added some basic features: a) named access list and b) nat. The access list was permitting all test traffic. Nat was not actively natting any packets.
  On Cisco IOS Release 12.4(24)T4, there was no packet droppage and thruput was as expected. On Cisco IOS Release 15.1(3)T, there was packet droppage (as seen on a traffic generator and also on the router in the form of “ignored” packets). Thruput was diminished by at least 10%.

- CSCtn87834
  Symptoms: Platform: Cisco devices crash during normal operation with the following message:
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 7669B0C data B0D0B0D chunkmagic 0 chunk_freemagic 100 -Process= "<interrupt level>". ipl= 1,
  Conditions: This symptom is observed on Cisco 7200 devices running Cisco IOS 12.4(24)T4.
  Workaround: There is no workaround.
- **CSCtn97267**
  Symptoms: Router crash in CCE code
  Conditions: This symptom occurs on an ISRG2 during normal operation.
  Workaround: There is no workaround.

- **CSCtn98633**
  Symptoms: IP phones lose registration with CUCME on a Cisco IAD887 after some usage.
  Conditions: This symptom is observed when transfer, call waiting, and other scenarios that involve MoH are present.
  Workaround: Disable MoH.

- **CSCto08904**
  Symptoms: RTP operations fail to run when using multiple operations.
  Conditions: When more than 16 RTP operations are running, operations start failing due to scaling issues.
  Workaround: There is no workaround.

- **CSCto10485**
  Symptoms: Mediatrace fails to activate all the sessions.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCto13338**
  Symptoms: When a PSTN phone is calling an IP Phone that is forwarded to a PSTN destination, the call is placed but no audio is present. The same symptom occurs with a blind transfer to external destinations.
  Conditions: This symptom is observed when the **voice-class codec X offer all** command and transcoders are used with the Cisco UBE.
  Workaround:
  - Use the **codec XXXX** command instead of the **voice-class codec X offer all** command
  - Perform a consultative transfer instead of a blind transfer.

- **CSCto31255**
  Symptoms: A router crashes at fair-enqueue.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCto38553**
  Symptoms: Iosips sends rst to a client on some http sessions with a printer after working for a few hours. Once the symptom occurs, it continues until the iosips configuration is removed from the interface.
  Conditions: This symptom is observed on a Cisco 3945 with an iosips configuration.
  Workaround: Remove and reapply the iosips config on the interface.

- **CSCto52353**
  Symptoms: Multilink bundles are not removed after clearing the vpdn session in LAC.
Conditions: This symptom is observed when a VPDN/L2TP tunnel is established between the client and the LNS.
Workaround: There is no workaround.

- CSCto52575
  Symptoms: A Cisco 7200 router crashes after unconfiguring tcp and rtp under the iphc-profile.
  Conditions: This symptom is observed on a Cisco 7200 running Cisco IOS Release 15.2(0.11)T.
  Workaround: There is no workaround.

- CSCto53119
  Symptoms: The VC stays down.
  Conditions: This symptom is observed after the following sequence:
  4. xconnect is configured on an SVI and the EoMPLS VC is up
  5. remove xconnect, remove SVI
  6. add the same vlan on VPLS VC via V-E
  Workaround: Remove and add back the VLAN in “down” state using the switchport allowed vlan command.

- CSCto54850
  Symptom: IP Phones fail to register with SRST GW after CCM Fallback to GW while testing call-forward and call-transfer scenarios.
  Conditions: This symptom is observed on an SRST GW running with failed image.
  Workaround: There is no workaround.

- CSCto55852
  Symptoms: A Cisco 2821 router crashes due to block overrun.
  Conditions: This symptom is observed when the router is acting as a fax gateway.
  Workaround: There is no workaround.

- CSCto63268
  Symptoms: A Cisco IOS router configured as a VoIP MGCP gateway interworking with Cisco Unified Communications Manager (CUCM - Callmanager) may experience an unexpected reload.
  Conditions: This symptom has been observed
  - in Cisco IOS Release 15.1T while attempting to parse the ccm config being pushed down
  - when using a digital (T1/E1) module interface when the MGCP PRI configuration is being pushed to the gateway from CUCM using the ccm-manager config command.
  Workaround: Either disable the T1/E1 configuration from CUCM or remove the ccm-manager config command. It may be possible to manually configure the MGCP with the PRI backhaul commands.

- CSCto63809
  Symptoms: A Cisco 3945 router is unable to receive updates from another router.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.
- **CSCto70421**
  Symptoms: Throughput performance drops between Cisco IOS Release 15.1(3)T and Release 15.1(4)M.
  Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.1(3)T to Release 15.1(4)M.
  Workaround: There is no workaround.

- **CSCto76888**
  Symptoms: A PSTN user calls up on a specific number which is directed to the IVR response via the Cisco 2800 GW router, but the PSTN user cannot hear anything due to the codec payload mismatch.
  Conditions: This symptom is observed when the first preference sent to a Cisco 2851 for an IVR announcement is the G.729ab codec.
  Workaround: Change the preference of the codecs so that G.729a is the preferred codec from the MGX.

- **CSCto83077**
  Symptoms: IPIPGW is not found in zone, though registered, when invia outvia is used for remote zone.
  Conditions: This symptom is observed with the incoming LRQ to GK with IPIPGW from the remote zone.
  Workaround: There is no workaround.

- **CSCto84268**
  Symptoms: TCP connections will take a longer time or will not work if PAT is enabled with two dialer links.
  Conditions: PC---fa0/1-7200-Vi 1.1---DSLAM---Di0---1841-f0/0---PC-Vi1.2---DSLAM---Di1--| The Cisco 1800 router has two dialer interfaces and NAT will point to Dialer 0 interface as the source address, but packets will leave the Dialer 1 interface with a source address of Dialer 0. If the ISP has enabled RPF check, then it will drop the packets coming out of the Dialer 1 interface.
  Workaround: Shut down one of the dialer interfaces.

- **CSCto85479**
  Symptoms: A Cisco 3945 router running EHWIC-4ESG claims itself to be the STP root for all active vlans. The Cisco 3945 router is not participating in STP root bridge election.
  Conditions: This symptom is observed on a Cisco 3945 router running Cisco IOS Release 15.1(4)M. Interfaces gi0/3/0-1 are on an EHWIC-4ESG card. The symptom was observed on an EHWIC-4ESG; data is not available for other HWIC cards.
  Workaround: There is no workaround.

- **CSCto96445**
  Symptoms: A router reloads while unconfiguring/configuring “call-router h323-annexg.”
  Conditions: This symptom is observed when “neighbor ip address” is configured.
  Workaround: There is no workaround.

- **CSCtq06497**
  Symptoms: Prefix not received at the remote end even after radius passes.
  Conditions: Conditions are unknown at this time.
Workaround: There is no workaround.

- **CSCtq12007**
  Symptoms: When removing tunnel protection from one tunnel, other tunnels sharing the same profile and the same source interface stop working.
  Conditions: This symptom affects multipoint GRE over IPsec tunnels (DMVPN) tunnels that are sharing the same ipsec profile (with keyword “shared” at the end of the tunnel protection statement), and are using the same interface as a source.
  Workaround: There is no workaround.

- **CSCtq15936**
  Conditions: This symptom is observed with Cisco IOS Release 12.4(24)T2 and Release 15.0(1)M4.
  Workaround: There is no workaround.

- **CSCtq17444**
  Symptoms: A Cisco AS5400 crashes when performing a trunk call.
  Conditions: This symptom is observed in Cisco IOS Release 15.1(3)T and on Cisco routers acting as voice gateways for H323.
  Workaround: There is no workaround.

- **CSCtq21234**
  Symptoms: A label is not removed after shutting down the link.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCtq22924**
  Symptoms: WSMA code does not allow more namespaces to be added to the SOAP envelope. Namespaces should be in the SOAP envelope in order for the CWMP agent to interwork with third-party ACS servers.
  Conditions: This symptom is observed with interworked third-party ACS servers that expect a dslforum namespace in the SOAP envelope. As per the TR-069 standard, the SOAP message must carry a private namespace in the SOAP envelope (xmlns:cwmp="urn:dslforum-org:cwmp-1-0">).
  Workaround: There is no workaround.

- **CSCtq23708**
  Symptoms: An active PGW crashes when deleting pdp, due to low mem with service records.
  Conditions: This symptom is observed when the pdp are cleared using the clear command and the SCU timeout happens.
  Workaround: There is no workaround.

- **CSCtq24733**
  Symptoms: A VXML gateway crashes with an unexpected exception to CPU: vector C.
  Conditions: This symptom is observed when MRCP is enabled.
  Workaround: There is no workaround.
- **CSCtq26270**
  Symptoms: HSRP packets are forwarded on STP blocked ports.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCtq30376**
  Symptoms: An SGW reloads for a dual APN with multiple MCBs under one user when the DDN message is tied to one of the MCBs. If this MCB is deleted, the crash occurs after n3t3 timeout.
  Conditions: This symptom is observed when the DDN message has been sent for the pdp.
  Workaround: There is no workaround.
  Further Problem Description: Since the DDN message is a user-level message, it should not be tied to any one MCB because that MCB can be freed before the DDN Ack is received or the n3t3 timeout occurs.

- **CSCtq36192**
  Symptoms: Cisco IOS with Zone Based Firewall crashes the router.
  Conditions: The issue is seen when modifying the parameter map as shown below:
  ```plaintext
  parameter-map type regex slim no pattern [^x80]
  ```
  Workaround: There is no workaround.

- **CSCtq36742**
  Symptoms: DmVPN DHCP does not work with a tunnel interface configured under a VRF on spoke.
  Conditions: This symptom is observed when vrf is configured.
  Workaround: There is no workaround.

- **CSCtq38474**
  Symptoms: A router running Cisco IOS may crash due to a bus error.
  Conditions: This crash is related to the forwarding of MPLS traffic. Additional conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCtq39602**
  Symptoms: The DMVPN Tunnel is down with IPSEC configured. The `show dmvpn` from the spoke shows that the state is “IKE.”
  Conditions: This symptom is observed after heavy traffic pumps from the DMVPN hub to the spoke for a period of time ranging from a few minutes to a couple of hours.
  Workaround: There is no workaround.

- **CSCtq40469**
  Symptoms: EEM policy registration fails.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCtq41512**
  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/No Shut will bring the PRI layer 1 to “Active” and layer 2 to “Multi-frame established.”
Caveats

Conditions: This symptom is observed when “voice-class busyout” is configured and the controller TEI comes up before the monitored interface.

Workaround: Remove the “voice-class busyout” configuration from the voice port.

- CSCtq48481

Symptoms: The following syslog and traceback are observed under high stress conditions with 300k subscriber sessions with MEF functionality enabled on the gateway and a QoS-profile (MBR/GBR):

```
SAMI 4/8: 000056: Jun 8 23:10:31: %SAMI-4-UNEXPECTED: Unexpected condition: Could not delete Hash-Entry -Process= "GTP Management", ipl= 0, pid= 124, -Traceback= 0x461C9520z 0x461D0A18z 0x461D3014z 0x455CDFD00z 0x455DD1888z 0x461DD820z 0x461DD890z 0x455DCAEF8z 0x455DD600z 0x455DCD4D0z 0x455DCDEC0z 0x442FC234z 0x4598BB78z 0x4598F27Cz
```

Conditions: This symptom is observed while maintaining the rate profile for given MBR/GBR values with a granularity of 2.7kbps for all subscriber sessions. The rate profile reference count (num_of_pdps) will wrap around after creating 65535 under each PPC (TCOP). When PDP are deleted after wrapping around the reference count, the syslog and traceback will be observed.

Workaround: Disable MEF functionality on the gateway or under an access-point configuration.

- CSCtq49325

Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

Conditions: This symptom is observed only when there are multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

Workaround: Redundant LANs may not be necessary. If they are required and if mutual redistribution is done, then while performing a graceful shutdown, sufficient time should be given for one process to be shut down completely before executing the second `shutdown` command. This should resolve the problem.

Problem Description: In a normal scenario, a zombie drdb or path entry (a temporary drdb entry that is deleted as soon as processing of the packet is complete) would be created only for the reply message. Due to redundancy in the LAN and the EIGRP processes in this scenario, a query sent on one interface comes back on the other interface, which causes this zombie entry creation for the query also. In the query function flow, it is expected that this zombie entry will not be deleted immediately; rather, it is to be deleted only after a reply for the query is sent successfully. At this point, before a reply is sent, if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However, if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed; the flow continues and the prefix itself is deleted. This causes a dangling path to exist without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to a crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths before deletion. Similar conditions will occur if the packetization timer expiry is not kicked in immediately to send the drdbs threaded to be sent, and a topology shutdown flow executes first.

- CSCtq51271

Symptoms: The web pages may not load, and the browser displays the following error: “Internet Explorer cannot display the webpage.” The following display is seen on the console:

```
*May 23 13:12:13.734: %FW-6-DROP_PKT: Dropping tcp session <X.X.X.X:80> <Y.Y.Y.Y:port> with ip ident 0
```

Conditions: This symptom is observed in Cisco IOS with the URL trend filter enabled.

Workaround: Refresh the webpage, or remove the IP of the specific website from being inspected.
- **CSCtq51554**
  Symptoms: A Cisco 881 router crashes during normal operation, but not much information is available in the crashinfo.
  Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T3 and earlier versions.
  Workaround: There is no workaround.

- **CSCtq55173**
  Symptom: A Cisco device crashes with NAT configured. SIP appears to be translated through NAT. However, some cases report that the crash is still present after redirecting SIP traffic elsewhere.
  Conditions: This symptom is observed when the `clear ip nat translation *`, `clear ip nat translation forced`, or `clear crypto ipsec client ezvpn` command is entered.
  Workaround: There is no workaround.

- **CSCtq56727**
  Symptoms: Bulk call failures occur during heavy traffic loads, followed by a gateway crash. The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP and other processes. Entering “sh proc mem sorted” shows continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway are constant.
  Conditions: This symptom is observed when the SIP trunk in Cisco Unified Communications Manager points to the gateway, is configured with DTMF signaling type as “no preference,” and the SIP gateway is configured with dtmf relay as sip-kpml.
  Workaround: There are two workarounds:
  1. Set the DTMF signaling type as “OOB and RFC 2833” in the Cisco Unified Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
  2. Configure “dtmf-relay rtp-nte” at the SIP gateway dial-peer configuration instead of “sip-kpml.” The Unified Communications Manager is configured with “no preference.”

  In order to recover from the crash, the gateway router must be reloaded.

- **CSCtq57330**
  Symptoms: A Cisco device crashes while processing calls.
  Conditions: This symptom is observed when H323 is being used.
  Workaround: There is no workaround.

- **CSCtq58364**
  Symptoms: NBAR sees IPsec packets on a DMVPN tunnel interface.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCtq59326**
  Symptoms: Flexible NetFlow stops working after some time.
  Conditions: This symptom is observed on a Cisco 3945 running Cisco IOS Release 15.1(3)T with Flexible NetFlow.
  Workaround: Reload the router.

  Further Problem Description: The “high watermark” value becomes 4294967295 with “current entries” close to that; “flows added” minus “flows aged” is close or equal to “cache size.”
Caveats for Cisco IOS Release 15.2(1)T

- **CSCtq59923**
  Symptoms: OSPF routes in the rib point to an interface that is down/down.
  Conditions: This symptom is observed when running multiple OSPF processes and with filtered mutual redistribution between the processes. When pulling the cable on one OSPF process, the OSPF database will clear, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.
  Workaround: Configure “ip routing protocol purge interface.”

- **CSCtq60799**
  Symptoms: A Cisco router crashes due to a memory corruption with the following error,
  ```
  %SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count
  ```
  Conditions: This symptom is observed when using a hardware crypto accelerator (VSA module).
  Workaround: There is no workaround.

- **CSCtq62069**
  Symptoms: A Cisco gateway crashes during CVP load testing.
  Conditions: This symptom is observed when a CVP Mixed Call-Flow test is run with 900 calls. The gateway crashes and a crash file is produced.
  Workaround: There is no workaround.

- **CSCtq63625**
  Symptoms: A WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4, is not getting trained with third-party DSLAMs unless the “line rate” is configured manually.
  Conditions: This symptom is observed on a WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4.
  Workaround: There is no workaround.

- **CSCtq63838**
  Symptoms: A Cisco 2921 router crashes with the following traceback:
  ```
  May 1 20:50:00.513: ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528:
  unkn -Traceback= 0x24A19810z 0x24A5DC8Cz 0x24A4A560z 0x24DF6618z 0x24DF6BBCz
  0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
  May 1 20:50:00.553: ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528:
  unkn -Traceback= 0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz
  0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
  May 1 20:50:00.553: %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer =
  315556E0. -Process= "DSMP", ipl= 0, pid= 306, -Traceback= 0x246EBB2Cz 0x24719984z
  0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
  0x233DEA40z 0x233DEA24z 23:50:00 UTC Sun May 1 2011: TLB (load or instruction fetch)
  exception, CPU signal 10, PC = 0x2581FB94
  ```
  Conditions: This symptom is observed with a Cisco router running Cisco IOS Release 15.0(1)M3 and with the DSMP process
  Workaround: There is no workaround.

- **CSCtq64153**
  Symptoms: When a PPPoE service-name is configured on an ATM interface or subinterface, the CLI is accepted but not applied.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.
Caveats

- **CSCtq67517**
  Symptoms: gh-sip.jar missing in locale-ja_IP-Japanese-8.6.2.4.tar
  Conditions: This symptom is observed when applying the Japanese locale in the Cisco SIP IP Phone 8961. gh-sip.jar file is missing in the CME-locale-ja_IP-Japanese-8.6.2.4.tar.
  Workaround: There is no workaround.

- **CSCtq70847**
  Symptoms: A Cisco 2900 series device fails to transmit a DCS message for T38 to RightFax.
  Conditions: This symptom is observed when T38 v0 is configured on the gateway, and with the following topology: PSTN---T1 CAS---2950---T38/SIP---RightFax IOS: c2951-universalk9_npe-mz.SPA.151-3.T1
  Workaround: There is no workaround.

- **CSCtq74389**
  Symptoms: When using an SVI interface as an L2TPv3 termination, the SVI interface unexpectedly floods an unknown unicast packet.
  Conditions: This symptom is observed when an SVI interface is used as an L2TPv3 termination.
  Workaround: Use a routed port instead of an SVI.

- **CSCtq74610**
  Symptom: A PGW crashes while sending the “modify command failure” message.
  Conditions: This symptom is observed when the Modify Bearer Command procedure is exercised under a load of 200 create-session-requests per second, and 200 modify bearer commands per second are performed simultaneously, with a lag of 60 seconds in between for a specific session.
  Workaround: There is no workaround.

- **CSCtq75008**
  Symptoms: A Cisco 7206VXR crashes due to memory corruption.
  Conditions: This symptom is observed under the following conditions:
  - the device is working as a server for L2TP over IPSec
  - encryption is done using a Cisco C7200-VSA
  - more than two clients are connected
  If client sessions are kept up for about a day, the router would crash.
  Workaround: There is no workaround.

- **CSCtq76005**
  Symptoms: Configuring “atm route-bridge ip” on MPLS-enabled ATM interface forces the router to punt all incoming MPLS packets to the CPU.
  Conditions: This symptom is observed when RBE is configured on an MPLS-enabled ATM interface.
  Workaround: Remove RBE.

- **CSCtq77024**
  Symptoms: Metrics collection fails due to an invalid DVMC runtime object handle.
  Conditions: This symptom occurs when the transport layer is not passing up an interface type that is acceptable to DVMC.
Caveats for Cisco IOS Release 15.2(1)T

Workaround:
1. remove and reschedule the mediatrace session
2. remove and reconfigure the mediatrace responder

- **CSCtq80858**
  Symptoms: A router crashes randomly at various decodes.
  Conditions: This symptom is observed when MACE and IP SLA TCP-based probes are configured.
  Workaround: There is no workaround.

- **CSCtq84313**
  Symptoms: A router hangs and then crashes due to a watchdog timer expiry.
  Conditions: This symptom is observed when IP SLA probes are configured, and then the configuration is replaced with one that has no IP SLA probes.
  Workaround: Reset the ip sla.

- **CSCtq84350**
  Symptoms: High memory utilization occurs in the IPS process.
  Conditions: This symptom is observed when Cisco IOS Release 12.4(24)T3 is upgraded to Cisco IOS Release 12.4(24)T5. Even with the same IPS configuration, the IPS process is utilizing 11 Mb more memory.
  Workaround: There is no workaround.

- **CSCtq85327**
  Symptoms: CCM-CCM Call forward cases fail when the Cisco UBE is in flow-around mode.
  Conditions: This symptom is due to a glare condition when the Cisco UBE receives and sends UPDATE message at the same time.
  Workaround: Disable “update caller-id” under “voice service voip.”

- **CSCtq85728**
  Symptoms: An EHWIC-D-8ESG card is causing an STP loop.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- **CSCtq85875**
  Symptoms: A device crashes in ipsec_dp_delete_sa when clear cry sess is entered.
  Conditions: This symptom is observed with a flexvpn configuration.
  Workaround: There is no workaround.

- **CSCtq89267**
  Symptoms: A router crashes or gets stuck.
  Conditions: This symptom is observed when the “debug ccsip messages” is enabled and call transfer is performed on a sip phone.
  Workaround: Avoid using “debug ccsip messages.”

- **CSCtq90054**
  Symptoms: A Cisco IOS router fails to recognize Skype-application traffic.
  Conditions: This symptom is observed after configuring PfR to control Skype traffic.
Caveats

Workaround: There is no workaround

- CSCtq90577
  Symptom: The router crashes when removing netflow.
  Condition: Conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCtq92650
  Symptom: A DMVPN Tunnel is not selecting the right source interface.
  Condition: The symptom is observed when Multi-link Frame-relay creates more than one subinterface with the same name.
  Workaround: There is no workaround.

- CSCtq92655
  Symptom: A DSP reset occurs with c5510_NO_RING_DESCRIPTOR errors.
  Condition: Conditions are unknown at this time.
  Workaround: There is no workaround.

  Further Problem Description: A DSP crash-dump showed that Cisco IOS is either not taking packets from DSP, or there is corruption of the HPI buffer pointer update.

- CSCtq92940
  Symptom: An active FTP transfer initiated from a Cisco IOS device used as a client may hang.
  Condition: This symptom is observed when an active FTP connection is used (for example, “no ip ftp passive” is present in the configuration) and there are device configuration or communication issues between the Cisco IOS device and the FTP server that, while allowing control connections to work as expected, stop the data connection from reaching the client.
  Workaround: Use passive FTP (default) by configuring “ip ftp passive.”

- CSCtq94509
  Symptom: A memory leak occurs in the “Dead” process.
  Condition: This symptom is observed on a Cisco 3845 running Cisco IOS Release 12.4(24)T5 or Release 12.4(24)T1.
  Workaround: None to stop the leak. However, monitoring “show memory stat” (processor pool, free column) will show free memory. Reload the router before the memory drops too low.

  Further Problem Description: “Show proc mem sorted” may show the “Dead” process holding more and more memory. In at least one case, the leak rate was 20-40Mb/day.

- CSCtq96329
  Symptom: Router fails to send withdraws for prefixes, when “bgp deterministic-med” is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.
  Condition: This symptom can happen only when “bgp deterministic-med” is configured.
  The following releases are impacted:
  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
Caveats

- Cisco IOS Release 15.2(1)T

Workaround: Disable deterministic med in the network/AS by issuing the `no bgp deterministic-med` command and then the `clear ip bgp *` command or hardreset of BGP session to remove any stale prefixes.

It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtq97723

Symptoms: A Cisco 3945 router may have performance issues (lower throughput) due to overruns.

Conditions: This symptom is observed with a steady bi-directional 64-byte ICMP stream. With Cisco IOS Release 15.0(1)M2, at 283Mbps = 37.16% wire rate of 1 gig, overruns began to increment. With Cisco IOS Release 15.1(4)M, at 206Mbps = 27.09% wire rate of 1 gig, overruns began to increment.

Workaround: There is no workaround.

- CSCtq97991

Symptom: An ADSL interface fails to re-train when the command line “dsl enable-training-log” is configured.

Conditions: This symptom is observed in the following:

1. Cisco 800, 1900, and 2900 devices, but the symptom could affect other software platforms
2. Cisco IOS Release 15.1(2)T, Release 15.1(2)T1 and Release 15.1(3)T3, but not in Cisco IOS Release 15.0(1)M4.

Workaround: The symptom is resolved after removing “dsl enable-training-log.”

Further Problem Description:

1. When “dsl enable-training log” is not configured, the HWIC trains up to the DSLAM with no problem; even after unplugging the cable and reconnecting it, the HWIC still comes up.
2. When “dsl enable-training log” is configured, after unplugging the cable and reconnecting it, the HWIC fails to come up. The CD LED does not blink and the following error message appears:

   "No retrain. sleep 20 seconds"

- CSCtr00381

Symptoms: A PRI interface goes down and cannot make a call after reload.

Conditions: This symptom is observed when the `modem firmware location` command is configured for using specific firmware for PVDM2-24DM.

Workaround: Re-insert the cable and shut/no shut the controller; this might clear the symptom temporarily. Or, delete the `modem firmware location` command.

- CSCtr01595

Symptoms: A Cisco AS5350XM router experiences a “software forced crash.”

Conditions: This symptom is observed on a Cisco AS5350XM used as a VXML Gateway and running Cisco IOS Release 15.1(3)T.

Workaround: Keep the number of active calls to 150 or less.
- **CSCtr03624**
  Symptoms: An incorrect “calling-station-id” is displayed during DHCP accounting.
  Conditions: This symptom is observed when accounting is triggered by the DHCP relay. It is not seen when accounting is triggered using the DHCP server.
  Workaround: Use a DHCP server to start accounting.

- **CSCtr07471**
  Symptoms: The following symptoms are observed:
  - on a Cisco 2800 router with HWIC cards and 2 ports connected to a Cisco 2960 switch (one in an STP blocking state), after 4-5 days of operation (more or less), the HWIC hangs and no traffic is forwarded via the card.
  - “show cdp neighbor” entered on the router displays the Cisco2960 switch, whereas when the same is entered on the switch, no neighbors are shown.
  - a shut/no shut on either the switch interface or the HWIC ports does not resolve the issue.
  Conditions: These symptoms are observed under the following conditions:
  - speed and duplex are matching on both sides (the issue is found even when the speed and duplex are set to auto)
  - the output rate for the interface on the HWIC card towards the switch shows 0 packet rate
  Workaround: Reload the router.

- **CSCtr07508**
  Symptoms: A crash is observed several times for a period of time. This crash occurs after enabling WAAS on the interface.
  Conditions: Conditions are not determined. Router is reloaded, no traffic is flowing through the router, or special configuration is done. This is seen several times in regression during a period of time, then ceases to happen in newer versions. Crash may be released with previous configuration on the router. It is not consistent.
  Workaround: There is no workaround.

- **CSCtr11030**
  Symptoms: An SGW reloads.
  Conditions: This symptom is observed when an SGW and a PGW are out of sync with respect to default bearers. Multiple Modify Bearer Responses are received from the PGW with a “Context Not found” error.
  Workaround: There is no workaround.

- **CSCtr11274**
  Symptoms: A backup clock is missing.
  Conditions: After the primary clock switches over, the new primary clock does not have a backup clock.
  Workaround: There is no workaround.

- **CSCtr11620**
  Symptoms: In a simple HSRP setup with Cisco 2900 devices, ping to a virtual IP intermittently fails.
  Conditions: This symptom is observed with a Cisco 2911 device.
  Workaround: Replace the Cisco 2900 series device with a Cisco 1800 series or a Cisco 1941.
• CSCtr13172
  Symptoms: Using the **configure replace** command causes the router to crash.
  Conditions: This symptom is observed when mediatrace and performance monitoring along with DMVPN are configured on the router.
  Workaround: There is no workaround.

• CSCtr14227
  Symptoms: Peer1 current-data metric set to default is not matching baseCost.
  Conditions: This issue is seen in routers loaded with Cisco IOS 15.1(2)T3.1
  Workaround: There is no workaround.

• CSCtr15040
  Symptoms: MCID is not clearing DSP resources when it receives the ISDN disconnect with PI.
  Conditions: Conditions are unknown at this time.
  Workaround: Remove the MCID script to release the DSP resources.

• CSCtr15518
  Symptoms: One-way audio occurs after transfer by the Cisco Unity auto attendant or IP phone SIP (PSTN) -- CUBE -- SIP -- CUCM -- Unity AA -- IP phone or SIP (PSTN) -- CUBE -- SIP -- CUCM -- IP phone -- blind transfer -- IP phone
  Conditions: This symptom is observed when a SIP trunk from the PSTN returns an IP address 0.0.0.0 when the connection is made inactive.
  Workaround: Enable pass-thru content sdp under voice service voip/sip.

• CSCtr16857
  Symptoms: Windowing in IKEv2 is broken.
  Conditions: This symptom is observed due to an error condition in auth exchange that causes the delete message to not be sent because of incorrect windowing:
  "No room in peer window request is throttled: Current Req = 2 Next Req = 1"
  Workaround: There is no workaround.

• CSCtr18559
  Symptoms: An unallocated/unassigned number is received from the PBX but, as a response, the gateway sends a network congestion notice back to the PBX. The gateway rejects the call with 4#, when it should send a 7#.
  Conditions: This symptom is observed only when the country “Brazil” is configured. When the country is set to “itu,” 5# is sent, which is correct for an unallocated/unassigned number.
  Workaround: There is no workaround.

• CSCtr18574
  Symptom: H323-H323 video calls fail with cause code 47; the following errors are seen:
  Received event H225_EV_H245_FAILED while at state H225_WAIT_FOR_H245
  cch323_send_passthru_out: Send passthru message retcode 15
  Conditions: This symptom is observed when H323-H323 video calls fail to establish an H245 media connection.
  Workaround: There is no workaround.
- CSCtr18985
  Symptoms: The CEF adjacency for a Frame Relay point-to-point circuit is incomplete, causing traffic passing through the router to drop.
  Conditions: This symptom is observed after reloading the router.
  Workaround: Flap the serial interface, or disable CEF on the serial interface or globally.

- CSCtr20300
  Symptoms: An SA negotiation test is failing for ipsec_core script; the SA should enter idle state after entering the `show crypto isakmp sa` command.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCtr20762
  Symptoms: When the router is reloaded, the following tracebacks are seen:
  Conditions: This symptom is observed with L3 VPN encapsulation IP. When the `aaa accounting system default` command is not used, the symptom does not occur.
  Workaround: Clear ip bgp * or disable the aaa accounting system.

- CSCtr21296
  Symptoms: The following messages are seen continuously on the router console:
  Conditions: The issue is seen after disabling the hardware crypto engine.
  Workaround: There is no workaround.

- CSCtr22683
  Symptoms: The EIGRP flaps.
  Conditions: This symptom is observed when tunnel protection is configured on a GRE tunnel.
  Workaround: There is no workaround.

- CSCtr25127
  Symptoms: When switching between ATM and 3G interfaces, the following traceback is observed.
  Conditions: This symptom is observed when switching between ATM and 3G interfaces.
  Workaround: There is no workaround.

- CSCtr25734
  Symptoms: A router crashes.
Conditions: This symptom is observed when a router reloaded with a BRI interface is brought up in start-up configuration.

Workaround: There is no workaround.

- CSCtr26018
  Symptoms: A Key Server crashes while unconfiguring VRF.
  Conditions: This symptom is observed during the removal of access-lists.
  Workaround: There is no workaround.

- CSCtr26117
  Symptoms: An authorized client gives its user credentials, but the password expiry rejects the pin and prompts the client to resubmit the pin.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCtr26144
  Symptoms: The UUT 5 second output packet rate falls out of 70/130% range while testing the PPPoE/VMI feature.
  Conditions: This issue is seen in routers running Cisco IOS Release 15.2(0.19)T0.1
  Workaround: There is no workaround.

- CSCtr26373
  Symptoms: An interface bounces and after coming back up, hangs and does not pass traffic. The Rx ring is stuck and all packets coming into the interface are counted as “input errors.” The interface will still show “up/up” in the “show interface” output.
  Conditions: This symptom is observed on a Cisco 3900. This may be seen at random times and has thus far occurred after an interface bounce.
  Workaround: Bounce the interface again to restore service.

- CSCtr26681
  Symptoms: QoS pre-classify fails for vpn traffic classification.
  Conditions: This symptom is observed when classification is based on an inner IP header.
  Workaround: Configure classification using ToS.

- CSCtr28594
  Symptoms: Load calculation fails on a VMI interface with high CDR, High traffic occurs while testing the PPPoE/VMI feature.
  Conditions: This issue is seen in routers running Cisco IOS Release 15.2(0.19)T0.1
  Workaround: There is no workaround.

- CSCtr28701
  Symptoms: A local server does not get an ip address from the remote server via IPCP.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCtr29460
  Symptoms: The dead memory on a Cisco 3845 router is holding up memory. The memory being held is constantly increasing.
Conditions: “sh memory dead” reveals significant amount of memory allocated for:

- SSH Process
- State Machine Instance
- TCP Remote Shell

Workaround: There is no workaround.

- **CSCtr29914**
  
  Symptoms: A Cisco 3945 crashes.
  
  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(4)M.
  
  Workaround: There is no workaround.

- **CSCtr31153**
  
  Symptoms: Packet decryption seems to fail with manual crypto maps configured on an interface.
  
  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.2(0.19)T0.1
  
  Workaround: There is no workaround.

- **CSCtr31578**
  
  Symptoms: Variable and inaccurate NTP sync results occur on 3945 and 3945E, leading to a few-second time drift every 24 hours.
  
  Conditions: This symptom is observed on the Cisco 3945/3945E under normal operation.
  
  Workaround: Configure "no ntp."

- **CSCtr32498**
  
  Symptoms: Input/output packet counts display double the expected value on “show interface output.”
  
  Conditions: This symptom is observed with an NM-16ESW card and not on the ports on the motherboard.
  
  Workaround: There is no workaround.

- **CSCtr33856**
  
  Symptoms: Tracebacks and/or crash occurs @ mace_monitor_waas_command:

```plaintext
Jul 5 21:08:54.635: %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 218959117 for chunk 6527D73C, data D0D0D0D -Process= "Exec", ipl= 0, pid= 373 -Traceback= 23054C68z 2238121Cz 223877F0z 22397A24z 2376B0FCz 2376B0E0z or %SYS-2-FREEBAD: Attempted to free memory at 4F, not part of buffer pool -Traceback= 24F4EA90z 23789608z 237758E4z 23054C68z 2238121Cz 223877F0z 22397A24z 2376B0FCz 2376B0E0z %SYS-2-NOTQ: unqueue didn’t find 4F in queue 28275D8C -Process= "Exec", ipl= 4, pid= 374 or watchdog crash following the above, with decodes pointing to mace_monitor_waas_command
```

Conditions: This symptom is observed after on-the-fly changes to mace policies and classes.

Workaround: There is no workaround.

- **CSCtr35456**
  
  Symptom: A router crash occurs at datalist_next while configuring mld proxy with PIM disabled.
  
  Conditions: This symptom is observed on Cisco IOS Release 15.2(1.2)T.
  
  Workaround: Start PIM (e.g., enable ipv6 multicast-routing) before configuring mld host-proxy.
Caveats

- **CSCtr35913**
  Symptoms: 200 OK response is deferred at incoming SIP leg. Possible Tracebacks due to accessing NULL1 memory.
  Conditions: Applicable for SIP-SIP calls in Cisco IOS images where the bad code fix CSCto72992 is present.
  Workaround: There is no workaround.

- **CSCtr38330**
  Symptom: A Cisco router may reload after configuring and unconfiguring ATM PVCs several times.
  Conditions: This symptom is observed on a Cisco 3825 running Cisco IOS Release 15.1(3)T1.
  Workaround: There is no workaround.

- **CSCtr40091**
  Symptoms: A call is not recorded.
  Conditions: This symptom is observed after a few days of the load.
  Workaround: There is no workaround.

- **CSCtr40568**
  Symptoms: Blind transferring an incoming call from PSTN back out to another PSTN number via a Cisco UBE results in one-way audio.
  Conditions: This symptom is observed in Cisco IOS Release version 15.1(2)T.
  Workaround: Revert to Cisco IOS Release 15.0(1)M1ES.

- **CSCtr41626**
  Symptoms: A Cisco 1941 and Cisco 2911 with 512MB memory fail to netboot via FTP due to Address Error (load or instruction fetch) exception following verification of the digital signature.
  Conditions: This symptom is observed on a Cisco 1941 or Cisco 2911 with 512MB memory and flash, and running Cisco IOS Release 15.1(4)M.
  Workaround: Boot the image directly from flash.

- **CSCtr41941**
  Symptoms: A DSP crash on occurs on a Cisco 3945 gateway when sending T38 fax with ECM disabled.
  Conditions: This symptom is observed on PVDM3 with ECM enabled, and in Cisco IOS Release 15.1.3T1
  Workaround: There is no workaround.

- **CSCtr42341**
  Symptoms: A crash occurs at task_execute_prep.
  Conditions: This symptom is observed on a Cisco 800 series router configured with BFD.
  Workaround: There is no workaround.

- **CSCtr43255**
  Symptoms: HWIC-3G-CDMA-V will not activate.
  Conditions: This symptom is observed with OTASP activation.
  Workaround: There is no workaround.
• CSCtr43993  
Symptoms: A router is crashing with CPUHOG messages and WATCHDOG TIMEOUT  
Conditions: This symptom is observed when Netflow is configured.  
Workaround: Disable Netflow.

• CSCtr45484  
Symptom: A router reloads while unconfiguring telephony service.  
Conditions: This symptom is observed with Cisco IOS Release 15.1(03)T1.5  
Workaround: There is no workaround.

• CSCtr46004  
Symptoms: When changing the “match” command the router reloads with a bus error.  
Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T10.  
Workaround: There is no workaround.

• CSCtr46577  
Symptoms: Dropped calls, informational (non-crash) MGCP tracebacks, ISDN signaling issues.  
Conditions: This symptom is observed with bad DSP hardware.  
Workaround: This issue is rarely seen. It results when there is a hardware problem with a DSP channel, and then signaling resources are assigned to the channel. There is currently no workaround except to replace the defective DSP module.

• CSCtr46815  
Symptoms: With some MACE CLI configurations, WAAS does not pick up any packets.  
Conditions: Conditions are unknown at this time.  
Workaround: There is no workaround.

• CSCtr46854  
Symptoms: A PPP multilink between a Cisco ISR G2 and a Cisco ASR1K crashes the ISR.  
Conditions: This symptom is observed on a Cisco ISR G2.  
Workaround: Remove authentication on the serial interface on the Cisco ASR1K.

• CSCtr47084  
Symptoms: Changing zone from multilink interface and replacing config with test config crashes the router.  
Conditions: This symptom is observed when traffic is running.  
Workaround: There is no workaround.

• CSCtr48480  
Symptom: A Cisco router may crash after “show gateway” is entered.  
Conditions: This symptom is observed on a Cisco 3825 running Cisco IOS Release 12.4(24)T4. The problem is rare in that most instances this command will not trigger a crash.  
Workaround: Do not enter “show gateway.”

• CSCtr49868  
Symptoms: A Cisco UBE crashes.
Conditions: This symptom is observed when the Cisco UBE is a Cisco 3945 running Cisco IOS Release 15.1.4M1.

Workaround: There is no workaround.

- CSCtr50008
  Symptoms: A Cisco UBE does not pass the reason header.
  Conditions: This symptom is observed with the following topology:
  Phone - Multiple vendor switches - Cisco UBE - Cisco UBE - CUCM 8.6 - Phone
  Workaround: Configuration had both a copy option under sip-profiles as well as allowing the reason header pass-through. Removing the copy option and just using the pass-through corrected the problem. However, the resulting reason header is not formatted as expected.
  Further Problem Description:
  Call flow: Routine call from vendor phone A to Cisco UBE - Cisco UBE to Cisco phone A
  Flash Override Call from vendor phone B to Cisco UBE - Cisco UBE to Cisco phone
  A Routine call is preempted as expected between the Cisco phone A and vendor phone A, and the Flash Override call is up between Cisco phone A and vendor phone B
  However, Cisco UBE is not passing to vendor phone A a reason header for the call termination. CUCM is sending the reason code to the Cisco UBE, but the Cisco UBE is not sending it along.

- CSCtr50118
  Symptoms: A router crashes.
  Conditions: This symptom occurs when presence feature is turned on.
  Workaround: There is no workaround.

- CSCtr52047
  Symptoms: A one-way audio issue occurs in SRST mode.
  Conditions: This symptom is observed under the following conditions:
  - when a Cisco 3925 is in SRST mode
  - internal calls are not affected
  Workaround: There is no workaround.
  Further Problem Description: Call setup is working fine, but RTP packets are not sent to the IP phone from the Cisco 3925. The phones fall into SRST, and the caller from PSTN can hear voice from IP phone, but the IP phone cannot hear voice from the PSTN. From the trace, the voice packets get received by the ephone packet handler layer, but from the phone statistics, no voice packet is received.

- CSCtr53265
  Symptoms: ISDN layer 1 is in deactivate state.
  Conditions: This symptom is observed with a WIC-1B-U-V2 card on a Cisco 2801.
  Workaround: There is no workaround.

- CSCtr53903
  Symptoms: One-way voice occurs, where POTS cannot hear VOIP.
  Conditions: This symptom is observed on a Cisco 3945 running Cisco IOS Release 15.1.2(T2) PVDM3 DSPware 26.8.1
Caveats for Cisco IOS Release 15.2(1)T

Resolved Caveats—Cisco IOS Release 15.2(1)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCs174976
  Symptoms: When MPLS-tagged packets are punted to MSFC CPU at a high rate, incoming interface hold-queue can fill up, and interface will be throttled. No packets are processed from throttled interfaces (until interface is unthrottled). If control plane protocols are running on throttled interfaces (especially with aggressive short timeouts), frequent throttling can lead to instabilities (such as BGP session loss, OSPF adjacency flaps, HSRP failovers, BFD neighbor less, etc.).
  Conditions: This symptom occurs when MPLS-tagged packets are punted to MSFC CPU at a high rate, incoming interface hold-queue can fill up, and interface will be throttled.
  Workaround: A certain level of stability can be gained by increasing hold queues on interfaces in questions. Also reducing the rates and duration of the traffic puniting to MSFC CPU will help.

- CSCtb72734
  Symptoms: DHCP OFFER is not reaching the client when the unicast flag is set.
  Conditions: This symptom occurs only on ASR devices where creation or removal of the ARP entry does not maintain sequential ordering. As a result, the packet could arrive at the forwarding plane after the ARP entry has already been removed or before the ARP entry has been created.
  Workaround: There is no workaround.

- CSCtc11266
  Symptoms: The router undergoes a bus error crash. Before the crash, the following error messages are displayed:
  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
  %SYS-4-SNMP_WRITENET: SNMP WriteNet request.
  %ALIGN-1-FATAL: Illegal access to a low address
  Conditions: This symptom is observed on a router running Cisco IOS Release 12.4(22)T1 that is used as a zone-based firewall with no routing and VPN configured.
  outside--ASA firewall------gig-IOS firewall-gig------inside network
  Workaround: There is no workaround.
Caveats for Cisco IOS Release 15.2(1)T

- CSCtd23069
  Symptoms: A crash occurs because of a SegV exception after configuring the ip virtual-reassembly command.
  Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 or Cisco IOS Release 12.4(24)T2.
  Workaround: There is no workaround.

- CSCtd87072
  Symptoms: IOSD restart seen.
  Conditions: The symptom is observed when changing tunnel mode on scaled IPSec sessions.
  Workaround: There is no workaround.

- CSCtd90030
  Symptoms: A Cisco 2851 router may crash with a bus error.
  Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.
  Workaround: There is no workaround.

- CSCtf39056
  Symptoms: RRI route will not be deleted even after IPsec SA has been deleted.
  Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.
  Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

  
  
  "configure terminal ! event manager applet SR_000000526 event timer cron name SR_000000526 cron-entry "0 3 * * *" action 1 cli command "en" action 2 cli command "reload" ! end


- CSCth03648
  Symptoms: Cisco 2960 and 3750 series switches running Cisco IOS Release 12.2 (53)SE1 may crash.
  Conditions: This symptom is observed if two traps are generated by two separate processes, and if one process suspends and the other process updates some variables used by the first process.
  Workaround: Disable all snmp traps.

- CSCth11006
  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:
  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol
  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.
  Cisco has released free software updates that address these vulnerabilities.
This advisory is posted at
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCth20018
  Symptoms: On a Cisco ISR G2 or Cisco 8xx product line, unconfiguring a subinterface (via config CLI, for example, `no interface g0/0.100` or `no interface atm0/0.100`) may sometimes crash the system.
  Conditions: This symptom occurs during basic configuration.
  Workaround: Do not unconfigure a subinterface.

- CSCti16649
  Symptoms: GETVPN GM reregisters.
  Conditions: This symptom is seen when any ACL is added or removed from the key server.
  Workaround: There is no workaround.

- CSCti48504
  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.
  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.
  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

- CSCti64685
  Symptoms: User may not be able to configure SLA MPLS configuration.
  Conditions: This symptom occurs when the router is booted up and may be random.
  Workaround: There is no workaround.

- CSCti87194
  Symptoms: The last fragment causes a crash because of an invalid zone value.
  Conditions: This symptom occurs when a Big IPC message is fragmented. Then, the last fragment causes the crash because of an invalid zone value.
  Workaround: There is no workaround.

- CSCti4921
  Symptoms: During the stress test of EzVPN, many messages are observed on the console like the following:
  `%PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT: IOS thread disabled interrupt for 11 msec`
  The EzVPN server is configured for dVTI and dynamic crypto maps. The stress test consists of bringing up and tearing down close to 1700 EzVPN clients (1250 dVTI and 450 dynamic cmap) clients.
  Conditions: This symptom is seen on a Cisco ASR 1006 router with RP2/FP20 combo with EzVPN clients coming in on GigE interfaces and on the latest XE3.2 throttle build. Many messages are seen on the console followed by tracebacks.
Caveats

Workaround: There is no workaround.

- CSCtj21045
  Symptoms: Header compression decodes RTP timestamp incorrectly.
  Conditions: This issue occurs mainly with IPHC format compression interacting with older IOS releases.
  Workaround: Use IETF format compression.

- CSCtj23189
  Symptoms: Packet drops on low rate bandwidth guarantee classes even if the offered rate is less than guaranteed rate.
  Conditions: This happens only when extremely high rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with 3 classes: one with 16kbps, second one with 1Mbps, and the third one with 99Mbps.
  Workaround: There is no workaround.

- CSCtj30155
  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:
  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload
  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.
  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCtj46670
  Symptoms: IPCP cannot complete after dialer interface is moved out of Standby mode. CONFREJ is seen while negotiating IPCP.
  Conditions: The symptom is observed when a dialer interface has moved out from standby mode.
  Workaround: Reload the router.

- CSCtj55624
  Symptoms: A router crashes upon entering the show crypto ruleset command.
  Conditions: This symptom is seen when version 6 crypto maps are configured.
  Workaround: Do not run the show command.

- CSCtj78966
  Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.
  Conditions: This symptom is seen when IKEv2 SA DB WAVL tree is getting corrupted if we fail to insert the SA due to some error, for example, PSH duplication.
  Workaround: There is no workaround.

- CSCtj87846
  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.
Caveats for Cisco IOS Release 15.2(1)T

Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.
Workaround: Do a shut/no shut on PfR master or PfR border.

- CSCtj94510
  Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and 4 SA dual per session, a crash happens on Crypto_SS_process.
  Conditions: This symptom occurs when sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and four SA dual per session.
  Workaround: There is no workaround.

- CSCtj94589
  Symptoms: With the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF and four SA dual per session, in unconfigured testbed after end of the IXIA traffic, crash happens at “no vrf” under “crypto isakmp profile”.
  Conditions: This symptom is seen with the configuration of 1000 VRFs (fvrf!=ivrf), with one IKE session per VRF and four SA dual per session.
  Workaround: There is no workaround.

- CSCtk12122
  Symptoms: A Cisco 7200 router may crash after clearing the SAs while using the IKE keepalive feature.
  Conditions: This symptom occurs when the IKE keepalive feature is turned on, and the user executes a clear crypto session command or a clear crypto sa command.
  Workaround: There is no workaround.

- CSCtk18330
  Symptoms: MSCHAPv2 auth fails when matching the user/password pair is configured.
  Conditions: This symptom is observed when matching the user/password pair is configured.
  Workaround: There is no workaround.

- CSCtk31401
  Symptoms: A Cisco router crashes when the SSH session from it is exited.
  Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.
  Workaround: There is no workaround.

- CSCtk67073
  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.
  Cisco has released free software updates that address this vulnerability.
  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla.

- CSCtk67709
  Symptoms: The AnyConnect 3.0 package does not install correctly on the Cisco IOS headend. It fails with the following error:
ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432-k9.pkg
SSLVPN Package SSL-VPN-Client (seq:1): installed
%Error: Invalid Archive

Conditions: This symptom is observed with AnyConnect 3.0.
Workaround: There is no workaround.

• CSCtk74660
Symptoms: The Network Time Protocol (NTP) tries to re-sync after the server clock changes its time and after the NTP falls back to the local clock.
Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.
Workaround: There is no workaround.

• CSCtk83638
Symptoms: Client gets assigned an IP address from an incorrect pool when it reconnects with a different profile.
Conditions: This symptom is observed in a setup where two clients are behind a NAT router. When one client connection is broken and the server is not made aware of this, and the client reconnects with a different group, the IP address assigned is not from the correct pool.
Workaround: There is no workaround.

• CSCtl00995
Symptoms: A Cisco ASR1K with 1000 or more DVTIs may reboot when we do shut / no shut on the tunnel interfaces or the tunnel source interface.
Conditions: This symptom is observed when all the DVTIs have a single physical interface as a tunnel source.
Workaround: Use a different tunnel source for each of the DVTIs. You can configure multiple loopback interfaces and use them as a tunnel source.

• CSCtl20993
Symptoms: Router crashes during IPsec rekey.
Conditions: The conditions for this crash are currently unknown.
Workaround: There is no workaround.

• CSCtl45684
Symptoms: A Cisco device may crash due to “CPU Signal 10” preceded by the following messages in the logs:

ASSERTION FAILED: file "../hwic/shdsl_efm_if_hwic_shdsl_efm_io.c", line 726
ASSERTION FAILED: file "../hwic/shdsl_efm_if_hwic_shdsl_efm_io.c", line 30

Conditions: This symptom is observed only when the HWIC-4SHDSL-E card is present in the router.
Workaround: There is no workaround.

• CSCtl54415
Symptoms: A Cisco router or switch may reload.
Conditions: This symptom is experienced on multiple platforms when single-connection timeout is configured under an aaa group server, and there is no TACACS key configured:

aaa group server tacacs+ <NAME> server-private x.x.x.x single-connection timeout 2
server-private x.x.x.x single-connection timeout 2 ip tacacs source-interface Loopback0 (no tacacs-server key configured)
Caveats

Workaround: Either configure the correct matching key or do not configure single-connection timeout.

- CSCtt58005
  Symptoms: Accounting delay start is sent before any NCP has been negotiated, with “aaa accounting delay-start” configured. According to PRD, accounting start should not be sent until first NCP has been negotiated.
  Conditions: This symptom occurs when “aaa accounting delay-start” is configured.
  Workaround: There is no workaround.

- CSCtt71478
  Symptoms: In an HA system, the following error message is displayed on the standby RP and LC: "OCE-DFC4-3-GENERAL: MPLS lookup unexpected"
  Conditions: This symptom is observed on standby/LC modules when you bring up both the RP and standby/LC routers with or without any configuration.
  Workaround: There is no workaround.

- CSCtt73564
  Symptoms: The same address is allocated for multiple IAIDs.
  Conditions: This symptom is observed when a client has been configured to send multiple IAIDs in a single request.
  Workaround: There is no workaround.

- CSCtt78285
  Symptoms: In VRF configuration, we are not able to add rd after deleting rd configuration once:
  A-SUP5-6509E#sho run | be vrf ip vrf CUST1 rd 1:1 route-target export 1:1 route-target import 1:1 mdt default 239.39.39.39
  A-SUP5-6509E(config)#ip vrf CUST1 A-SUP5-6509E(config-vrf)#no rd 1:1 % "rd 1:1" for VRF CUST1 scheduled for deletion
  After two hours, we try to add the rd again.
  A-SUP5-6509E(config)#ip vrf CUST1 A-SUP5-6509E(config-vrf)#rd 1:1 % Deletion of "rd" in progress; wait for it to complete A-SUP5-6509E(config-vrf)#
  Conditions: This symptom is seen in a VRF configuration with rd.
  Workaround: Remove VRF configuration and add again.

- CSCtt82517
  Symptoms: For the Cisco ME3600 and Cisco ME3800, the following licensing errors are seen, leading to license manager failure at bootup:
  %SCHED-7-WATCH: Attempt to lock uninitialized watched semaphore (address 0).
  -Process= "Init", ipl= 4, pid=
  Conditions: This symptom is seen when a Cisco ME3600 or Cisco ME3800 license- based image is loaded off mcp_dev_nile.
  Workaround: Use whales-universal-mz.

- CSCtt87067
  Symptoms: Priority class will drop traffic before explicit police rate is reached.
  Conditions: This symptom is observed on Cisco ISR platforms when strict priority with explicit police is configured.
Workaround: There is no workaround.

- **CSCtl92210**
  
  Symptoms: A router may crash when trying to show the sessions on responder while the session queue is being managed (removal).

  Conditions: This symptom occurs while new sessions are being provisioned or removed from mediatrace initiator side. The router can crash when trying to show the session objects on the responder while the session queue is being managed (removal) by first disabling the initiator using the `no mediatrace initiator force` command and then disabling responder with the `no mediatrace responder` command.

  Workaround: Do not disable initiator with the `no mediatrace initiator force` command and responder with the `no mediatrace responder` command in quick succession while the `show mediatrace responder session [brief | details]` command is not finished with output or in pause mode.

- **CSCtl94813**
  
  Symptoms: When using iLBC, the VG224 fails to play audio out the FXS port. The call uses iLBC when the analog phone on the VG224 attends a conference bridge. It causes one-way audio. When the IP capture is decoded from the VG224, the iLBC audio packet received and sent to the VG224 Fast Ethernet interface is clearly seen. For the same call, the PCM trace shows no audio in the RIN stream.

  Conditions: This symptom occurs with Cisco IOS Release 15.1(2)17T. As per the HPI logs, the Cisco IOS does not send any packets to the dsp:

  ```
  *Mar 10 23:36:54.988: //1944/9948BD1D87E7/HPI/[0/1:1]/hpi_receive_query_rx: Got RX stats Packet details: Packet Length=188, Channel Id=1, Packet Id=200 RX Packets=0: Signaling=0, ComfortNoise=0 Receive Duration=129180(ms): Voice=0(ms), FAX=0(ms) Packet Counts: OOSequence=0, Bad header=0, Late=0, Early=0 Receive inactive duration=129(ms)
  ```


- **CSCtl98132**
  
  Symptoms: XDR CPU hog may cause system crash.

  Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

  Workaround: There is no workaround.

  Further Problem Description: The crash can be avoided if the system has no double failure.

- **CSCtn02632**
  
  Symptoms: A MAB supplicant never gets authenticated and remains in RUNNING state.

  Conditions: This symptom is observed when a MAB supplicant connected to FA1 port of a Cisco 890 router remains in RUNNING state indefinitely after issuing a warm reload of router.

  Workaround: Use other FE ports if a warm reload is issued.

- **CSCtn04686**
  
  Symptoms: When MHSRP is configured and the hello packets are passing through Etherchannel, and the cables connected to the Etherchannel port are unplugged/plugged, the MHSRP hello packets are not received on the Etherchannel interface.

  Conditions: This symptom is observed on a Cisco 3845 router running Cisco IOS Release 15.0(1)M4.

  Workaround: Unplug/plug the cables.
- CSCtn08673
  Symptoms: A Cisco device crashes with tracebacks:
  08:56:31 gmt Fri Jan 14 2011: Unexpected exception to CPU: vector D, PC = 0x3CD7565
  %Traceback= 3CD7565 29D255AC 3D5602E 3D3A510 3D69BC2 3CC49C8 3CC2266 3CCD42B 3CCC96D
  Conditions: This symptom is observed on a Cisco 3900 running Cisco IOS Release 15.1(1)T1.
  Workaround: There is no workaround.

- CSCtn10507
  Symptoms: Tracebacks at fw_dp_base_process_new_pak & fw_dp_state_object_init_obj IPv6 routing and mediatrace do not come up.
  Conditions: This symptom is observed when FW with self zones is configured on the router.
  Workaround: There is no workaround.

- CSCtn10922
  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic, and in some cases, may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.
  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.
  Workaround: Configure the ip pim nbma-mode command on the point-to-point ATM subinterfaces.

- CSCtn18229
  Symptoms: A policy does not get suspended.
  Conditions: This symptom is observed if a policy is applied to fr-pvc, then the member link is flapped from the peer for mfr subint.
  Workaround: There is no workaround.

- CSCtn18437
  Symptoms: Crash seen @ qos_set_assign_pak_feature_object.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCtn18784
  Symptoms: Interface Tunnel 0 constantly sends high-bandwidth alarms.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCtn19027
  Symptoms: The show mediatrace responder sessions brief command crashes the router.
  Conditions: This symptom is observed on Mediatrace Responder when showing a stale session.
  Workaround: There is no workaround other than to avoid entering impacted show command.

- CSCtn19178
  Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working vrf “A” and a new local label will not be reassigned.
**Caveats for Cisco IOS Release 15.2(1)T**

**Caveats**

**Conditions:** This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused vrf “B”, including:

- the vrf interface, for example, `no interface Gi1/0/1.430`
- the same vrf process, for example, `no router ospf process id vrf vrf name`

Run the following commands to verify whether you are facing this issue:

- `show ip bgp vpnv4 vrf A subnet` (this is for the working vrf)
- `show mpls forwarding-table labels local label`

**Workaround:** To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

- `clear ip bgp mp-bgp neighbor soft in`
- `clear ip bgp mp-bgp neighbor soft out`

**Symptoms:** Packet loss is seen when the service policy is applied on the tunnel interface. The `show hqf interface` command output shows drops in a particular queue with the following:

`Scheduler_flags 177`

The above value of 177 indicates an ATM driver issue. Once the issue is seen, the tunnel interface transitions to the down state.

**Conditions:** This symptom is observed when the service policy is applied on the tunnel/GRE interface, and when the source of the tunnel interface is the ATM interface (hwic-shdsl)

**Workaround:** There is no workaround.

**Further Problem Description:** The above-described symptom is seen only with the SHDSL link.

**Symptoms:** Placing fax calls through c5510 DSP (NM-HDV2, etc.) using Voice over Frame Relay (VoFR) may trigger UNSUPPORTED CODEC messages on the console and possibly a WatchDog Timeout.

**Conditions:** This symptom is observed with Cisco IOS Release 15.1(2)T and Release 15.1(4)M.

**Workaround:** Use Voice over IP (VoIP) instead of VoFR, or use an older IOS release.

**Symptoms:** PLATFORM_EIGRP_TRACE_LOG_SIZE_IN_KB should not be hard coded to 20. The PLATFORM_VALUE_CRASH_BUFFER_SIZE is already defined as 20.

**Conditions:** Conditions are unknown at this time.

**Workaround:** There is no workaround.

**Symptoms:** With the pseudowire redundancy, after performing “clear xconnect all” on the remote primary peer, the VCs that switchover to the backup PWs are now in the standby state on the primary peer. However, they are in down state on the local node instead of standby state.

**Conditions:** This symptom occurs when performing “clear xconnect all” on the remote primary peer where initially all the VCs are in UP state.

**Workaround:** There is no workaround.

**Symptoms:** SDP PassThru + IPv6 to IPv4 Conversion is not working.
Conditions: This symptom is observed with Cisco IOS Release 15.1(3.22)T and Release 15.1(3)T.
Workaround: There is no workaround.

- CSCtn31333
  Symptoms: CPU utilization is high due to the process Net Background.
  Conditions: This symptom is observed on a router used for LNS with an L2TP application after upgrading to Cisco IOS Release 12.4(24T).
  Workaround: There is no workaround.

- CSCtn36227
  Symptoms: Alignment errors are seen at ipv6_checksum.
  Conditions: This symptom is seen when the GRE tunnel is configured with IPv6 ping sweep going across.
  Workaround: There is no workaround.

- CSCtn39632
  Symptoms: RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.
  Conditions: This occurs on a Cisco ASR 1000 series router configured for RSA key encryption with a keyring name having more than 8 characters.
  Workaround: Modify the keyring name to be less than 8 characters.

- CSCtn41793
  Symptoms: With IP session and traffic after OIR/SSO, the downstream traffic is not flowing.
  Conditions: This symptom occurs after OIR/SSO.
  Workaround: There is no workaround.

- CSCtn46263
  Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.
  Conditions: This symptom is observed during retransmissions and window throttling of requests.
  Workaround: There is no workaround.

- CSCtn51740
  Symptoms: Memory leak is seen in EzVPN process.
  Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.
  Workaround: There is no workaround.

- CSCtn52270
  Symptoms: CWMP is not coming up.
  Conditions: This symptom is seen because of the “alcdsl_get_wan_dsl_link_config” function.
  Workaround: There is no workaround.

- CSCtn53794
  Symptoms: A multilink PPP interface stays down after SSO.
  Conditions: This symptom is observed when the serial interfaces on an 8xCHT1/E1 are configured to be a part of a ppp multilink group and a redundancy force-switchover command is entered.
Workaround: There is no workaround.

- CSCtn55070
  Symptoms: Call-home http messages can hang and not be sent out.
  Conditions: This symptom is observed when call home is enabled and an http transport method is used. This symptom is timing-dependent and cannot be hit every time. In addition, this symptom is observed in telnet sessions.
  Workaround: Log in to the console port if a telnet session was used to send call-home http messages. Because the console is waiting on user-supplied information (More--), enter something into the console; the call-home process can then continue to execute.

- CSCtn55187
  Symptoms: Memory leaks are seen at ikev2_ipsec_add_proxy_to_list, ikev2_skeyseed_create, and ikev2_ios_get_ipv6_pak on the Cisco 2900 and Cisco 3900 platform routers respectively.
  Conditions: This symptom is seen after the test has been completed and while trying to check for the memory leaks when testing the Tunnel Protection for IPv6 feature.
  Workaround: There is no workaround.

- CSCtn61501
  Symptoms: CfmFlowRtpPayloadType does not return the correct value.
  Conditions: When CISCO-FLOW-MONITOR-MIB displays a flow carrying RTP information, it does not populate the correct value for the object cfmFlowRtpPayloadType.
  Workaround: Enter the show performance monitor status command. Entering this command will not make the object behave correctly, but it will provide an alternate way to see the value for the payload type.

- CSCtn61834
  Symptoms: NAT-T keepalive cannot send out cause NAT translation timeout.
  Conditions: This symptom is seen when the NAT translation table is getting timeout since no NAT keep alive message is received.
  Workaround: There is no workaround.

- CSCtn63109
  Symptoms: After reload or on a freshly upgraded router, Ping fails when the MTU is set above 1500 bytes on the FastEthernet 4-WAN interface of a Cisco 800 series router connected directly to another router.
  Router# ping 10.1.1.1 rep 5 df-bit size 1650 Type escape sequence to abort. Sending 5, 1650-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: Packet sent with the DF bit set . . . .
  Conditions: This symptom is only observed with Cisco IOS Release 15.0(1)M4 and is specific only to Cisco 800 series routers. To be specific, only the Cisco 881SRST router is found faulty with the IOS, that is, c880voice-universalk9-mz.150-1.M4.bin so far. This issue is consistently seen with subinterface configurations based on the Fa4 interface.
  Also, the following Traceback is noticed:
  *Feb 28 15:26:19.639: %LINK-4-TOOBIG: Interface FastEthernet4, Output packet size of 1664 bytes too big, -Traceback= 0x81056958z 0x81056EF8z 0x8112CBF4z 0x8200073Cz 0x82001264z 0x82001978z 0x8201BBF4z 0x8201C16Cz 0x8203F5C8z 0x8203FDACz 0x82D86B9Cz 0x81A1DC70z 0x819E6FD8z 0x819F6114z 0x8128C0CCz
  Workaround: Remove and reconfigure MTU on the interface.
CSCtn65060
Symptoms: A Cisco device crashes.
Conditions: This symptom is observed with Cisco IOS Release 15.0M and Release 15.1T when configuring “snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL.”
Workaround: Avoid using the snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL command.

CSCtn65130
Symptoms: The “evaluate” statement on an IPv6 ACL in Cisco IOS cannot be added after the “sequence” statement; for example,
```
%router(config)#ipv6 access-list test
%router(config-ipv6-acl)#evaluate REFLECTOUT ? sequence Sequence number for this entry <cr>
%router(config-ipv6-acl)#evaluate REFLECTOUT sequence 10 router
%sequence 10 evaluate REFLECTOUT
As this syntax is not accepted, when the router boots up this command is not applied, so it is lost on the running config.
```
Conditions: This symptom is observed when configuring IPv6 reflexive ACL on Cisco IOS.
Workaround: Manually re-enter the ACL with only the accepted syntax after boot.

CSCtn68117
Symptoms: The session command does not work on a Cisco 3000 series router that has become the master after a mastership change.
Conditions: This symptom is observed upon fail-over to slave.
Workaround: There is no workaround.

CSCtn68643
Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.
Conditions: This symptom occurs when configuring OSPFv3 IPsec authentication or encryption:
```
ipv6 ospf encryption ipsec spi 500 esp null sha1
1234123412341234123412341234123412341234
or ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd
```
Workaround: There is no workaround.

CSCtn70367
Symptoms: IPSEC key engine crashes at sessions setup.
Conditions: This symptom is seen when setting up sessions with the configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. The crash happens on IPSEC key engine. The crash occurs while UUT is establishing SAs that are requested. This issue is reproduced by clear crypto session on CES after all SAs are established.
Workaround: There is no workaround.

CSCtn72853
Symptoms: Crash/watchdog timeout occurs at udb_classify_child.
Caveats

Conditions: This symptom occurs due to various triggers like applying service-policy changes to complex level 2 or 3 policies where the same child/grandchild policy is used multiple times in the same parent.

Workaround: There is no workaround.

- CSCtn72939
  Symptoms: The L2tpv3 feature is not working on Cisco 1810 series platforms.
  Conditions: This symptom occurs with a Cisco 1812 running Cisco IOS Release 15.(0)M and later releases.
  Workaround: Configure bridge-group under that xconnect interface.

- CSCtn74169
  Symptoms: Crash by memory corruption occurs in the “EzVPN Web-intercept daemon” process.
  Conditions: This symptom is observed when EzVPN server pushes a long banner to the client after HTTP authentication using HTTP intercept.
  Workaround: Do not use long banner in HTTP intercept.

- CSCtn76183
  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.
  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.
  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

- CSCtn77211
  Symptoms: Spurious memory access occurs at cce_dp_ipc_cache_classify at bootup.
  Conditions: This symptom is observed when IPv6 SLA probes are configured, along with the firewall.
  Workaround: There is no workaround.

- CSCtn79475
  Symptom: A Cisco router reloads often due to stack overflow under some traffic conditions.
  Conditions: This symptom is observed when calls resulting in VOIPRTP media loop are seen.
  Workaround: There is no workaround.

- CSCtn82089
  Symptoms: Connectivity loss to PCs in data vlan occurs when connected to ports on a EHWIC-D-8ESG-P. PCs do not get IP address from DHCP server.
  Conditions: This symptom is observed when the EHWIC-D-8ESG-P interface is configured in the following order (portfast prior to voice vlan):
  
  Router(config-if)#switchport access vlan 100  
  Router(config-if)#spanning-tree portfast  
  Router(config-if)#switchport voice vlan 101  
  
  Workaround: Remove the portfast and voice vlan configuration and re-apply voice vlan prior to portfast.
  Further Problem Description: If the router is reloaded, it is possible that the portfast is applied first, leading to the connectivity loss.
- **CSCtn83520**
  Symptoms: VOIP_RTCP related traceback is seen.
  Conditions: This symptom is observed when IPIP gateways are involved.
  Workaround: There is no workaround.

- **CSCtn87012**
  Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.
  Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.
  Workaround: Pick up the phone during the ringing OFF cycle.

- **CSCtn87155**
  Symptoms: CoA sessions are not coming up.
  Conditions: This symptom is observed when some CLI commands that are called within shell function might fail if the shell programmatic APIs are used.
  Workaround: Manually use shell functions on the console.

- **CSCtn90630**
  Symptoms: Leaks occur at __be_udb_create_rtcg_p and __be_udb_remove_class_in_class_group or a crash occurs at __be_udb_pre_feature_unbind_child.
  Conditions: This symptom is observed with modification of complex 3 level QoS policy under certain scenarios.
  Workaround: There is no workaround.

- **CSCtn90673**
  Symptoms: The Cisco 887 router crashes when sending baby jumbo frames downstream over the VDSL line.
  Conditions: This symptom is observed when the VDSL interface, “interface e0”, is configured for PPPoE, a subinterface (that is, vlans), and an output service policy on interface e0. This issue is seen when an etherswitch interface is configured for trunking and baby jumbo frames or jumbo frames are sent downstream to the router. There is bidirectional traffic and the etherswitch vlan is then shut.
  Workaround: Do not send baby jumbo frames or jumbo frames downstream to the Cisco 887 router. Do not shut the etherswitch vlan interface(s) when the router is routing traffic.

- **CSCtn93891**
  Symptoms: Multicast traffic is getting blocked.
  Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.
  Workaround: There is no workaround.

- **CSCtn95344**
  Symptoms: After RPR downgrade from SRE2 CCO to SRE1 CCO, the standby RSP gets stuck in cold bulk and reboots every 50 minutes.
  Conditions: This symptom occurs after RPR downgrade from SRE2 CCO to SRE1 CCO.
  Workaround: Perform reload on the router.
Caveats for Cisco IOS Release 15.2(1)T

- **CSCtn96521**
  Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.
  Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.
  Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- **CSCtn97451**
  Symptoms: The bgp peer router crashes after executing the `clear bgp ipv4 unicast peer` command on the router.
  Conditions: This symptom occurs with the following conditions:
  
  ```
  Router3 ---ebgp--- Router1 ---ibgp--- Router2
  
  ROUTER1: -------- interface Ethernet0/0 ip address 10.1.1.1 255.255.255.0 ip pim sparse-mode !
  router ospf 100 network 0.0.0.0 255.255.255.255 area 0 ! router bgp 1 bgp log-neighbor-changes network 0.0.0.0 neighbor 10.1.1.2 remote-as 1 neighbor 10.1.1.3 remote-as 11 !
  
  ROUTER2: -------- interface Ethernet0/0 ip address 10.1.1.2 255.255.255.0 ip pim sparse-mode ! router ospf 100 redistribute static network 0.0.0.0 255.255.255.255 area 0 ! router bgp 1 bgp log-neighbor-changes network 0.0.0.0 redistribute static neighbor 10.1.1.1 remote-as 1 ! ip route 192.168.0.0 255.255.255.0 10.1.1.4
  
  ROUTER3: -------- interface Ethernet0/0 ip address 10.1.1.3 255.255.255.0 ip pim sparse-mode !
  router bgp 11 bgp log-neighbor-changes network 0.0.0.0 network 0.0.0.0 mask 255.255.255.0 redistribute static neighbor 10.1.1.1 remote-as 1 ! ip route 192.168.0.0 255.255.0.0 10.1.1.4
  
  Crash reproduce steps are as follows:
  1. Traffic travel from ROUTER3 to ROUTER2
  2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2
  
  Workaround: There is no workaround.
  
- **CSCto00318**
  Symptoms: SSH session that is initiated from a router that is running Cisco IOS Release 15.x may cause the router to reboot.
  Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.x.
  Workaround: For now, consider not initiating an SSH session from the Cisco router that is running a Cisco IOS Release 15.x train.

- **CSCto00796**
  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).
  Conditions: This symptom occurs when a new interface is provisioned inside a vrf and the configuration such that the connected routes are redistributed in the vrf. This redistributed route fails to tag itself with the RT when it reaches the peering PE(+RR)
  Workaround: Soft clear the peer that missed getting the RT.


- **CSCto02448**
  
  **Symptoms:** On doing an inbound route refresh, the AS-PATH attribute is lost.
  
  **Conditions:** This symptom is observed with the following conditions:
  1. The neighbor is configured with soft-reconfiguration inbound
  2. The inbound routemap is not configured for the neighbor
  3. The non-routemap inbound policy (filter-list) allows the path.

  **Workaround:** Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- **CSCto02712**
  
  **Symptoms:** DHCP client stops accepting IP address when ASR replies for arp packet of client’s IP address obtained via DHCP.
  
  **Conditions:** Some of DHCP clients that check for duplicate IP addresses before configuring a DHCP assigned IP address may reject IP address assignment.
  
  **Workaround:** Configure “no ip proxy arp” on a dhcp server-facing interface.
  
  **Further Problem Description:** The above workaround would work if the DHCP server/relay agent is directly on the client’s subnet and is not separated by an L2 technology that stops ARP (for example, a DSLAM).

- **CSCto03506**
  
  **Symptoms:** The Gigabit Ethernet 0/2 interface on Cisco 3900 platforms is not seen by applications using snmp.
  
  **Conditions:** This symptom is observed on Cisco 3900 platforms.
  
  **Workaround:** There is no workaround.

- **CSCto05108**
  
  **Symptoms:** A Cisco 7206 with VSA card is used as a GETVPN GM. After some time of operation, the router prints VSA-related traceback and completely stops encrypting/decrypting any traffic:

  ```%008720: Feb 24 11:11:01.674 GMT+5: VSA shim: crypto_ike_encrypt_callback ctx_next
  NULL -Traceback= 0x1BF4364z 0x3D38AE4z 0x3D007FCz 0x3CFA77Cz 0x3CFE108z 0x15829FCz
  0x15857ACz 0x1584800z 0x15822C8z 0x5580000z 0x1584E78z 0x1582384z 0x3D00DD8z
  0x5D00A64z 0x3D3852Cz 0x3D411B8oz```

  After that, all encrypted traffic is dropped. Crypto debugs (debug crypto isakmp, etc.) do not produce any messages. The only way to recover is to reboot the router.
  
  **Conditions:** This symptom is observed on a Cisco 7206 where a VSA card is used as a GETVPN GM and running Cisco IOS Release 15.0(1)M4 or Release 12.4(24)T3.
  
  **Workaround:** Disable encryption.

- **CSCto07586**
  
  **Symptoms:** An IPV4 static BFD session does not get established on a system which does not have IPv6 enabled.
  
  **Conditions:** This symptom occurs under the following conditions:
  - Create an IOS image that does not IPv6 enabled
  - Enable BFD on an interface
  - Configure an IPV4 static route with BFD routing through the above interface.

  The IPV4 BFD session does not get established, so the static route does not get installed.
Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- **CSCto08754**
  Symptoms: The crypto VTI interface with ip unnumbered VTI may experience input queue wedge. When the interface becomes wedged, all incoming traffic from the tunnel drops.
  Conditions: This symptom occurs when the crypto VTI interface becomes wedged.
  Workaround: There is no workaround.

- **CSCto09161**
  Symptoms: A Cisco router with MACE+NAT configuration crashes after a few hours of traffic.
  Conditions: This symptom is observed when both MACE+NAT are enabled on the interface.
  Workaround: There is no workaround.

- **CSCto10165**
  A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.
  Cisco has released free software updates that address this vulnerability.
  There are no workarounds available to mitigate this vulnerability other than disabling the Smart Install feature.
  This advisory is posted at [http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smart-install](http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-smart-install)

- **CSCto11025**
  Symptoms: When traffic streams are classified into multiple classes included with LLQ with qos-preclassify on the tunnel interface and the crypto map applied to an interface, packets are dropped on crypto engine on the Cisco 890 series router with buffers unavailable.
  Conditions: This symptom is observed when IPSec and QoS are used when qos-preclassify is on the tunnel interface and a crypto map is on the main interface.
  Workaround: Use tunnel protection or VTI instead of the crypto map on the interface.

- **CSCto12514**
  Symptoms: After turning a member link, multilink goes to suspense mode and it will not come back even after the member comes back.
  Conditions: This symptom is observed with an MPOL configuration.
  Workaround: Remove the MPOL configuration.

- **CSCto12825**
  Symptoms: The multilink policy cannot be removed.
  Conditions: This symptom is observed with MPOL configured; when multilink goes to suspension, the policy cannot be removed.
  Workaround: There is no workaround.

- **CSCto13254**
  Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error:
Hash verification failed for file <temp location of profile>

Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.

Workaround: Remove the profile from the Cisco IOS headend.

- CSCto14435
  Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.
  Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This issue is seen with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.
  Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.

- CSCto15278
  Symptoms: Tracebacks are seen at managed_chunk_low.
  Conditions: This symptom occurs when sending multicast traffic and using the `show memory debug leaks chunks` command.
  Workaround: There is no workaround.

- CSCto15361
  Symptoms: Active Supervisor crashes after removing the “router eigrp” configuration.
  Conditions: This symptom occurs when the Active Supervisor crashes while disabling the IPv6 router eigrp because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.
  Workaround: Modify the igrp2_procinfo_free function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto16319
  Symptoms: Traceback is thrown while starting Re-Auth timer and Re-auth always happens.
  Conditions: This symptom is observed when a Session-Timeout value from the RADIUS server is set to a high value which is rounded to a negative value in authenticator.
  Workaround: There is no workaround.

- CSCto16597
  Symptoms: When using the voluntary PPP feature with L2TP, a memory leak is seen. The leak is of AAA memory that is allocated on behalf of the voluntary PPP.
  Conditions: This symptom occurs when there is a disconnect of the L2TP or voluntary PPP connection.
  Workaround: There is no workaround.

- CSCto23807
  Symptoms: A Cisco device crashes when trying to transfer a call.
  Conditions: This symptom is observed with Cisco IOS Release 15.1(1)T2.
  Workaround: There is no workaround.
• ** CSCto24338**
  Symptoms: Router reload occurs due to the following bus error when the processor reads data from an invalid memory location:
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xXXXXXXXX
  Conditions: This symptom occurs with NAT+SIP.
  Workaround: Disable the NAT SIP multipart processing by executing the **no ip nat service allow-multipart** command.

• ** CSCto31265**
  Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.
  Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.
  Workaround 1: Delete/read the static route that generates Type7.
  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.
  Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

• ** CSCto34196**
  Symptoms: When two Cisco 3945E routers are connected to each other and an IPSec VPN tunnel is established between them, any kind of traffic passing through the VPN tunnel takes about 10 milliseconds as Round Trip Time in case the Onboard Encryption Engine is used.
  Conditions: This symptom occurs only when that traffic is encrypted by the Onboard Encryption Engine of Cisco 3945E (SPE250). After replacing the routers to Cisco 3945 (SPE150), the RTT is shorter than the one of Cisco 3945E.
  Workaround: Use software encryption.

• ** CSCto41165**
  Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit|deny** command, and then the **no ip extcommunity-list 55 permit|deny** command.
  Conditions: This symptom occurs when the standby router is configured.
  Workaround: There is no workaround.

• ** CSCto41173**
  Symptoms: A voice gateway crashes by TLB (store) exception with BadVaddr = 00000244.
  Conditions: This symptom is observed with a platform that acts as an H323 gateway and runs Cisco IOS Release 15.1(3)T.
  Workaround: Revert to Cisco IOS Release 12.4(20)T.

• ** CSCto42752**
  Symptoms: Removing the existing static policy and applying it back or adding the policy under that interface if it does not exist results in an error on standby.
  Conditions: This symptom occurs when customers use high availability.
  Workaround: Using the non-HA or standalone routine will fix the problem.

• ** CSCto43683**
  Symptoms: Suspended service policy is not re-enabled when MFR bundle link comes up.
  Conditions: This symptom is observed when the service policy is attached to MFR DLCI.
Workaround: There is no workaround.

- CSCto43776
Symptoms: The “shared” keyword does not work as expected on the second tunnel interface on a HUB with the first tunnel interface connecting to a dmvpn spoke and the second tunnel interface to point-to-point GRE peer.
Conditions: Conditions are unknown at this time.
Workaround:
1. Flap both T1 and T2
2. For T2 use a different ipsec profile. This ipsec profile should be using a different transform set (either different encryption protocol or different hashing protocol)
3. Configure the tunnel interfaces from scratch using the “shared” keyword

- CSCto43807
Symptoms: The secondary tower will resume the IP Address of the primary tower when the secondary tower has been incorrectly configured.
Conditions: This symptom is observed when the primary tower is incorrectly configured and is not up.
Workaround: Configure the secondary tower with the correct DNS name or IP Address.

- CSCto44016
Symptoms: After connectivity to the primary tower is lost, the secondary tower does not take over, and the following status is displayed:
```
#sh content-scan summ
Primary: <tower-primary-IP-address> (Up)*
Secondary: <tower-secondary-IP-address> (Up)
```
The primary tower is still showing as the active tower.
Conditions: This symptom is observed when connectivity to the primary tower is lost.
Workaround: Reload the router. After reload, the following status is displayed:
```
#sh content-scan summ
Primary: <tower-primary-IP-address>(Down)
Secondary: <tower-secondary-IP-address> (Up)*
```

- CSCto44581
Symptoms: The router crashes on high call volume.
Conditions: This symptom occurs on high call volume.
Workaround: There is no workaround.

- CSCto45019
Symptoms: The router crashes when you remove the dialer interface and read it and configure an IP address.
Conditions: This symptom occurs if you have continuous traffic passing through the router and going out of the dialer interface, and if you remove the dialer interface and read it and then configure an IP address.
Workaround: Before configuring an IP address, configure encapsulation ppp or frame-relay but not hdlc.
• CSCto46716
Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.
Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In "debug ip ospf spf", when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.
Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

• CSCto47524
Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder.
Conditions: This symptom is observed on a Cisco ASR 1002 router.
Workaround: Disable IP SLA on affected router, if possible.

• CSCto50255
Symptoms: A memory leak occurs while running UDP echo operation.
Conditions: This symptom is observed when an UDP echo operation successfully runs. Leak is seen on every 100th run of the UDP echo operation. Using the show memory debug leaks command will not capture this. The only way is monitoring and decoding the PC via the show processes memory pid command.
Workaround: There is no workaround.

• CSCto53332
Symptoms: A router configured for IPSEC accounting may display the following error message:
%AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
This does not seem to result in any impact apart from intermittently lost accounting messages.
Conditions: This symptom occurs when ipsec accounting is active.
Workaround: There is no workaround.

• CSCto55623
Conditions: This symptom is observed in Cisco IOS Release 15.2(6)PI16.
Workaround: There is no workaround.

• CSCto55708
Symptoms: A build error occurs due to a missing quotation mark (""") in a printf statement, only in dgs, due to compiler-specific issues.
Conditions: Conditions are unknown at this time.
Workaround: There is no workaround.

• CSCto60399
Symptoms: Ping is not working if GETVPN is enabled
Conditions: This symptom is observed if icmp/ip acl are configured on KS.
Workaround: There is no workaround.

- CSCto61098
  Symptoms: Incremental SNMP chunk-leaks are observed.
  Conditions: This symptom is observed when GETVPN is enabled on the interface.
  Workaround: There is no workaround.

- CSCto63954
  Symptoms: A router with GETVPN configurations is continuously crashing.
  Conditions: This symptom is seen with GETVPN-related configurations with fail-close feature activated.
  Workaround: There is no workaround.

- CSCto65352
  Symptoms: System crashes randomly when the Apex module is in the system.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

- CSCto68554
  The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.
  These vulnerabilities are:
  - Memory leak in Cisco IOS Software
  - Cisco IOS Software Denial of Service when processing specially crafted HTTP packets
  Cisco has released free software updates that address these vulnerabilities.
  Workarounds that mitigate these vulnerabilities are not available.
  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw

- CSCto69071
  Symptoms: Metrics collection fails due to invalid DVMC runtime object handle.
  Conditions: This symptom occurs when the transport layer is not passing up an interface type that is acceptable to DVMC.
  Workaround: There is no workaround.

- CSCto71744
  Symptoms: FXO interfaces with the cable-detect feature enabled will automatically transition to the off-hook state when no PSTN battery voltage is detected, and remain off-hook for a duration of up to 1 minute. This condition violates regulatory telecom standards in several countries, including but not limited to the USA and Canada.
  The failing clauses of regulatory standards are as follows:
  - TIA-968-B 5.1.11.3
  - TIA-968-B 5.1.12.3
  - Industry Canada CS-03 Part I, Issue 9 December 2010
Conditions: This symptom occurs when the FXO interface is up and the cable is connected to the PSTN. Any interruption of the PSTN battery to FXO induces the off-hook condition, and the port does not transition back to on-hook for up to 1 minute.

Workaround: Disable the cable-detect feature in the FXO <config-voiceport> prompt. You can enable the feature in topologies that are not subject to regulatory standards (that is, on-premise installations).

- CSCto72932
  Symptoms: Traceback is seen at ephone_create_dn.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround

- CSCto73151
  Symptoms: An RP resets.
  Conditions: This symptom is observed when the **sh ip nhrp** is entered to check mixed dmvpn and svti.
  Workaround: There is no workaround

- CSCto75350
  Symptoms: A crash occurs at udb_classify.
  Conditions: This symptom occurs when level 3 HQoS is configured. The second-level policy from under-class-default is removed. This is followed by traffic, either self-generated through IP SLA or possibly through data traffic traversing.
  Workaround: There is no workaround.

- CSCto76018
  Symptoms: ASR1000-WATCHDOG crashed after clear crypto session on CES.
  Conditions: This symptom is observed when sessions setting up with the configuration of 1000 vrf, 1 IKE session per vrf and 4 IPSec SA dual per session, hit the crash on ASR1000-WATCHDOG process while CES clear crypto session on CES after all SAs had been established.
  Workaround: There is no workaround.

- CSCto77537
  Symptoms: Calls between SME and Cisco UBE fail due to no audio path when the originating leg is G729r8 and the Cisco UBE preferred codec list contains g729br8.
  Conditions: This symptom occurs under the following conditions:
  - Cisco UBE ISR: Cisco 3845 running Cisco IOS Release 15.1(4)M
  - There is no audio path after call setup. The call either disconnects (case SIP-H323) or stays up without voice path (case SIP-SIP).
  The call flow is as follows:

  OriginatingCluster--> SAF SIP Trunk ---> SME ---> CUSP --> CUBE (originating) --> CUSP
  <----------> CUSP --> CUBE (Terminating) --> CUSP --> SME --> SAF H323 Trunk --->
  TerminatingCluster

  Cisco UBE codec configuration:

  voice class codec 1 codec preference 1 g729r8 codec preference 2 g729br8 codec preference 3 g711ulaw codec preference 4 g722-64

  Workaround 1: Remove the g729br8 codec in the voice-class codec config on the Cisco UBE to ensure that CUBE will offer only g729r8 in the outgoing offer.
Workaround 2: Change the Originating SME, SIP trunk to Originating Cisco UBE from DelayOffer to EarlyOffer.

Workaround 3: Configure a transcoder.

- **CSCto79015**
  Symptoms: If a connection fails to authenticate, the next http request sent by a client will sit in a redirect loop to the virtual IP for a URL whose authentication was previously aborted.
  Conditions: This symptom is observed when virtual-ip is configured and the first authentication fails.
  Workaround: There is no workaround.

- **CSCto80032**
  Symptoms: User group information sent to the ScanSafe tower is based on post-NATed IP.
  Conditions: This symptom is observed when configuring “content-scan out” on the egress interface.
  Workaround: There is no workaround.

- **CSCto80719**
  Symptoms: A Cisco 860 crashes.
  Conditions: This symptom is observed when applying tunnel protection on the tunnel interface.
  Workaround: Use a crypto map configuration.

- **CSCto81814**
  Symptoms: When SSH is attempted over an IKEv2 tunnel using ECDSA certificates, the router crashes.
  Conditions: This symptom is observed only when ECDSA certificates are used for IKEv2 and not with RSA certificates or with IKEv1.
  Workaround: There is no workaround.

- **CSCto86833**
  Symptoms: A router CPU spikes to 100 percent, leading to voice call failures, among other problems.
  Conditions: This symptom occurs with the Cisco 3945e router configured with SRST (call-manager-fallback) to the maximum supported capacity of 1500 phones, 2500 DNs with octo-line capability, and PRI interfaces controlled via ccm-manager. Under these conditions, MGCP call processing consumes significant amount of CPU. Even at 0.5cps MGCP call arrival rate, the router’s average CPU will be around 50 to 60 percent.
  Workaround: If possible, reduce the number of voice ports automatically generated by the number DNs and octo-line. Also, if possible, use dual-line support instead. The lower the number of voice ports, the lower the CPU impact of this defect. Use the `show voice port summary` command to view the total number of voice ports created on the router after SRST configuration.

- **CSCto88393**
  Symptoms: CPU hogs are observed on a master controller:
  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0), process = OER Master Controller.
  ```
  Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.
  Workaround: There is no workaround.
• CSCto88581
  Symptoms: The standby RP crashes following an interface configuration change.
  Conditions: This symptom is observed only when “ospf non-stop routing” is configured.
  Workaround: There is no workaround.

• CSCto88686
  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.
  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.
  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip

• CSCto92123
  Symptoms: Continuous tracebacks occur at both the ce_sw_encrypt_ipsec_packet and the encrypt_process.
  Conditions: This symptom is observed when switching a traffic profile in Ixia and removing a service-policy under the interface.
  Workaround: There is no workaround.

• CSCto92586
  Symptoms: Chunk leak seen at ipsec_dp_init.
  Conditions: Conditions are unknown at this time.
  Workaround: There is no workaround.

• CSCto98212
  Symptoms: When RIPng is removed from an interface from telnet and serial console sessions at the same time, it causes the routers to crash.
  Conditions: This symptom occurs when RIPng is configured on an interface and two users are connected using two different console sessions.
  Workaround: Do not configure the same RIPng through two different console sessions.

• CSCto98742
  Symptoms: A typo may cause a main interface to be deleted when there is no subinterface of the port-channel:
  ```
  %7609(config)#no inter port-channel 1.1
  ```  
The extra space between the interface and the subinterface numbers can cause all the port-channel 1 configurations to be deleted. Logical interface port-channel 1 and all sub-interfaces under this port-channel are deleted.
  Conditions: Conditions are unknown at this time.
  Workaround: Ensure the correct format is used with no extra spaces in the “no” form of the command.
• CSCto99523
   Symptoms: Convergence can take more time if there are a lot of vrf routes and aggregation is configured in many vrfs and massive route churn happens (for example, a session reset with RR).
   Conditions: Conditions are unknown at this time.
   Workaround: There is no functionality impact.

• CSCtq04117
   Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via Loop back. OSPF provides reachability to BGP next hop, and BFD is running.
   Conditions: This symptom occurs under the following conditions:
   1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT
   2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.
   Workaround: Use the `clear ip route vrf x` * command.

• CSCtq04404
   Symptoms: The browser goes into a redirect loop without prompting for authentication.
   Conditions: This symptom is observed when ip admission, virtual-ip and Basic/NTLM authentication methods are configured.
   Workaround: Remove virtual-ip configurations.

• CSCtq05636
   Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg. For example:
   Received: INVITE sip:1869863384**83782255010.253.24.35:5060 SIP/2.0
   Sent: INVITE sip:1869863384**83782255010.253.24.35:5060 SIP/2.0
   In Cisco IOS Release 15.1.3T1, the * character is not forwarded.
   Conditions: This symptom is observed when the Cisco UBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1.3T1.
   Workaround: Upgrade to Cisco IOS Release 15.1.3T or Cisco IOS Release 15.1(M4).

• CSCtq06538
   Symptoms: RP crash due to bad chunk in MallocLite.
   Conditions: Conditions are unknown at this time.
   Workaround: There is no workaround.

• CSCtq07222
   Symptoms: Non-RSVP to RSVP calls fail for iLBC codec in Voice class codec.
   Conditions: This symptom is observed with calls involving High density transcoding and Voice class codec with an iLBC codec.
   Workaround: Remove the iLBC codec from the Voice class codec.

• CSCtq07413
   Symptoms: A hardware crypto engine may fail to decrypt packets. An “invalid parameter” error is seen after decryption. Software encryption works fine.
   Conditions: This symptom is observed in Cisco IOS Release 12.4.15T6.
Workaround: Use software encryption.

- CSCtq09542
  Symptoms: A Cisco UBE responds with “481/Transaction does not exist” for CANCEL message.
  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M.
  Workaround: Use Tel URI instead of SIP URI.
  Further Problem Description: SP----(SIP)-----CUBE-----CUCM
  Basic Call Scenarios are working fine with one exception: Party A (outside SIP Network) is calling party B (CUCM Phone). B is ringing, A gets ring-back. Now A cancels the call (before B answers the call). A gets released, B continues ringing.

- CSCtq09712
  Symptoms: A Cisco ASR RP crashes due to L2TP management daemon:
  %Exception to IOS: Frame pointer 0xXXXXXXXXXXXX, PC = 0xZZZZZZZZZ IOS Thread backtrace: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = L2TP mgmt daemon
  Conditions: This symptom is observed with L2TP when clearing the virtual access interfaces.
  Workaround: There is no workaround.

- CSCtq09899
  Symptoms: The VXML gateway crashes.
  Conditions: This symptom occurs during the load test when the show mrcp client session active is used.
  Workaround: There is no workaround.

- CSCtq10356
  Symptoms: When video is enabled under a call manager profile, the Zone-Based Firewall SIP inspection engine will not create the RTP pinhole for voice.
  Conditions: This symptom is observed when video is enabled under the phone profile.
  Workaround: Disable video under the phone profile; the two options to disable are “Cisco Camera” and “Video Capabilities.”

- CSCtq10524
  Symptoms: A Cisco device may crash.
  Conditions: This symptom is observed when more than the recommended number of Mediatrace sessions (>255) is applied to one interface.
  Workaround: Keep the number of Mediatrace sessions below the recommended maximum per interface.

- CSCtq10684
  Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.
  Conditions: This symptom occurs when tunnel flap is observed before the crash.
  Workaround: A possible workaround is to reload the box.

- CSCtq14817
  Symptoms: Traceback or crash might happen when PPTP related traffics were passing through NAT configured device.
Caveats for Cisco IOS Release 15.2(1)T

Conditions: A race condition when PPTP packets were subjected to NAT, that might cause NAT to behave improperly and cause the issue.

Workaround: There is no workaround.

- CSCtq15247
  Symptoms: The router crashes when removing the virtual-ppp interface. The crash is more common if the l2tp session is flapping when the virtual-ppp interface is removed.
  Conditions: This symptom occurs if the l2tp session is flapping when the virtual-ppp interface is removed.
  Workaround: Remove the pseudowire command from under the virtual-ppp interface command before removing the interface.
  For example:

  LAC1(config)#interface virtual-ppp1
  LAC1(config-if)#no pseudowire
  LAC1(config-if)#exit
  LAC1(config)#no interface virtual-ppp1

- CSCtq18068
  Symptoms: An “autoqos:error” is seen when configuring auto QoS VoIP.
  Conditions: This symptom is observed in Cisco IOS Release 15.2(1)T.
  Workaround: There is no workaround.

- CSCtq21785
  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS-XE Release 15.1(2) S may crash upon performing a CRL check on an invalid certificate.
  Conditions: The conditions are unknown.
  Workaround: Turning off CRL check should stop the crash. It should be configured as:

  "revocation-check none"

  This will stop the CRL check of the peer certificate but should not be a long term solution.

- CSCtq24006
  Symptoms: DMVPN tunnels will not come up with an IPv6 address.
  Conditions: This symptom is observed if more than one tunnel is present on the spoke.
  Workaround: There is no workaround.

- CSCtq25682
  Symptoms: The router crashes after configuring “gw-accounting file”.
  Conditions: This symptom occurs if the router’s memory usage is already over 80 percent utilization, and after configuring “gw-accounting file”, the following log message is displayed:

  %VOICE_FILE_ACCT-4-MEM_USAGE_HI_WATERMARK: System memory on high usage (81/100).
  Stopping processing new event log for now.

  After this log, when the cdrflush-timer expires, the router crashes.
  Workaround: Do not enable “gw-accounting file” when the router’s memory utilization is already over 80 percent.

- CSCtq26057
  Symptoms: Multicast ping fails after manual SA is fixed.
  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T.
Caveats

Workaround: There is no workaround.

- CSCtq26892
  Symptoms: A Cisco UBE crashes @ sipSPI_ipip_IsHdrInHeaderList.
  Conditions: This symptom is observed with a PRACK-NO PRACK configuration on Cisco IOS Release 15.2(1)T.
  Workaround: There is no workaround.

- CSCtq27180
  Symptoms: After a Cisco IOS upgrade, any permanent licenses are erased and eval licenses do not work.
  Conditions: This symptom is observed only on IOS internal releases.
  Workaround: There is no workaround.
  Further Problem Description: The following LOG messages and errors are found:
  Mar 30 01:27:38.003: %LICENSE-2-LIC_STORAGE: Storage validation failed -Traceback= 604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z Mar 30 01:27:38.447: %LICENSE-2-VLS_ERROR:’VLSsetInstallLicenseStorage’ failed with an error - rc = 116 - ‘Error[136]: Specified license store doesn’t exists.’ -Traceback= 604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z

- CSCtq28151
  Symptoms: A bus error crash occurs.
  Conditions: This symptom is observed on a Cisco 3900 voice gateway running Cisco IOS Release 15.1(3)T1.
  Workaround: There is no workaround.

- CSCtq30686
  Symptoms: A Cisco router crashes in a Secure Device Provisioning (SDP) environment.
  Conditions: This symptom is seen when the Registrar router crashes when a client router submits an enrollment request that was previously stuck in “granted” status with the same fingerprint.
  Workaround: There is no workaround.

- CSCtq30875
  Symptoms: A Cisco router that is acting as an RA crashes in an SDP environment with CVO setup.
  Conditions: This symptom occurs during CVO enrollment request.
  Workaround: There is no workaround.

- CSCtq33102
  Symptoms: A Cisco router that is acting as an RA crashes in an SDP environment with CVO setup.
  Conditions: This symptom occurs during CVO enrollment request.
  Workaround: There is no workaround.

- CSCtq35297
  Symptoms: Cisco 880 images do not get compiled.
  Conditions: This symptom occurs during compilation of Cisco 880 images.
Caveats: There is no workaround.

- **CSCtq36726**
  - Symptoms: Configuring the `ip nat inside` command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned Virtual-access interface. The NAT functionality is thus broken, because the V-access interface does not get this command cloned from its respective VTEMP.
  - Conditions: This symptom is observed on Cisco ASR1006 (RP2/FP20) routers with ikev2 dVTI. This issue may be service impacting and is easily reproducible.
  - Workaround: Reconfigure the Virtual-template interface such that the `ip nat inside` command is applied first, followed by other commands.

- **CSCtq37579**
  - Symptoms: Enabling and disabling snmp-server traps crashes the UUT.
  - Conditions: This symptom is observed when disabling the snmp-server, then performing a write memory.
  - Workaround: There is no workaround.

- **CSCtq38303**
  - Symptoms: A policy is rejected with an insufficient bandwidth percent guarantee.
  - Conditions: This symptom is observed with bandwidth percentage guarantees.
  - Workaround: Do not configure bandwidth in percentages.

- **CSCtq42864**
  - Symptoms: A memory leak occurs @ sipSPI_ipip_UpdateSdpForPthru : Basic SDP Passthru Call.
  - Conditions: This symptom is observed with SDP PassThru Calls.
  - Workaround: There is no workaround.

- **CSCtq45553**
  - Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features.
    - Memory Leak Associated with Crafted IP Packets
    - Memory Leak in HTTP Inspection
    - Memory Leak in H.323 Inspection
    - Memory Leak in SIP Inspection
  - Workarounds that mitigate these vulnerabilities are not available.
  - Cisco has released free software updates that address these vulnerabilities.
  - This advisory is available at the following link:

- **CSCtq47428**
  - Symptoms: A Cisco router acting as an SRST may unexpectedly reload due to a bus error.
  - Conditions: This symptom is observed with phones registered to the SRST.
  - Workaround: There is no workaround.

- **CSCtq48228**
  - Symptom: A Cisco UBE crashes: Translate Redirect + 302 Consumption +SDP PassThru Scenario
Caveats

Conditions: Conditions are unknown at this time.
Workaround: Do not configure “SDP PASSTHRU.”

- CSCtq49408
  Symptoms: Analog phone calls (fxs) cannot be made with CME/SCCP.
  Conditions: This symptom occurs when SCCP support for FXS is missing in a Cisco IAD2435.
  Workaround: There is no workaround.

- CSCtq49860
  Symptoms: If an ISM VPN module is installed in the ISR G2 platform, we will exceed export limits without HSECk9 license installed.
  Conditions: This symptom is observed when an ISM VPN module is installed and enabled for crypto acceleration.
  Workaround: There is no workaround.

- CSCtq55723
  Symptoms: With Transport Control Protocol (TCP) and User Datagram Protocol (UDP), operations with VPN Routing and Forwarding (VRF) are not working.
  Conditions: This symptom occurs only with VRF.
  Workaround: Works without VRF.

- CSCtq59777
  Symptoms: A Cisco device crashes.
  Conditions: This symptom is observed when the `show mrcp client session history` command is entered.
  Workaround: Do not enter the `show mrcp client session history` command.

- CSCtq61850
  Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.
  Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.
  Workaround: There is no workaround.

- CSCtq62322
  Symptoms: On an SNR call, when the call is forward and connected to CUE after ringing to the remote target, nothing happens (for example, no CUE prompt occurs, and the user cannot leave voice mail).
  Conditions: This symptom is observed if the answer-too-soon timer is configured, the remote target is a pstn call, and the calling party is using a sccp phone.
  Workaround: There is no workaround.

- CSCtq64951
  Symptoms: The following message is displayed:
  \%CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license.
  The `show platform cerm` command output shows all tunnels in use by SSLVPN:
Caveats for Cisco IOS Release 15.2(1)T

OL-25471-04 Rev. P0

Number of tunnels 225 ... SSLVPN D D 225 N/A

The show webvpn session context all command output shows no or very few active sessions.

WebVPN context name: SSL_Context

WebVPN context name: SSL_Context

Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq75045

Symptoms: When a router is running FlexVPN-IKEv2 in auto-reconnect mode, IPSec SAs are not renegotiated properly after a clear crypto session command is entered. Entering the show crypto ikev2 client flexvpn command will indicate that the router is in a NEGOTIATING state.

Conditions: This symptom is observed on a router running FlexVPN on IKEv2 in auto-reconnect mode.

Workaround: Enter the clear crypto ikev2 client flexvpn command to clear the FlexVPN state and renegotiate the SAs successfully.

- CSCtq83257

Symptoms: A Cisco 870 platform router crashes while booting with an advipservices image.

Conditions: This symptom is observed on a Cisco 870 platform router running Cisco IOS Release 15.2(0.18)T and while booting with an advipservices image.

Workaround: There is no workaround.

- CSCtq86500

Symptoms: Crypto breaks non-encrypted traffic.

Conditions: This symptom is observed after migration to Cisco IOS Release 15.0(1)M6.

Workaround: Disable VSA and use software encryption.

- CSCtq96544

Symptoms: Application id is limited to 100.

Conditions: While configuring new applications, the application id allows values in the range 0-100 only.

Workaround: There is no workaround.

- CSCtr01957

Symptoms: The system crashes when “crypto engine slot 0” is entered.

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtr06926

Symptoms: CA Server goes to Disable State once Trustpoint authenticated.

Conditions: Conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtr25821

Symptoms: Cisco 800 series routers crash with the isdn leased-line BR10 128 command:

----- Unexpected exception to CPU: vector 1000, PC = 0x0 , LR = 0x8155A310 -----
Caveats

Conditions: Conditions are unknown at this time.
Workaround: There is no workaround.

- CSCtr26531
  Symptoms: When we disable ISM VPN accelerator using no crypto engine slot 0, the ISM VPN module is not disabled. Also, under high load the ISM VPN firmware download will fail.
  Conditions: This symptom is observed with an ISM VPN module and during high traffic loads.
  Workaround: There is no workaround.

- CSCtr37099
  Symptoms: RTCP Passthru does not work for IPv4 to IPv6 calls with two interfaces. The Cisco UBE does not send RTCP packets from the IPv6 interface.
  Conditions: This symptom is observed with two interfaces, and is not seen with only one interface.
  Workaround: Enable IPv6 on IPv4-only interface.

- CSCtr44686
  Symptoms: A crash occurs after matching traffic and resetting the connection using the following maps:

  ```
  policy-map type inspect smtp SMTP_L7_P1
  class type inspect smtp SMTP_L7_C1
  reset
  policy-map type inspect smtp SMTP_L7_P2
  class type inspect smtp SMTP_L7_C2A
  reset
  class type inspect smtp SMTP_L7_C2B
  reset
  ```
  Conditions: Conditions are unknown at this time.
  Workaround: Replace “reset” with “log.”
Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.2M&T. This documentation set consists of software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Use these release notes with the documents and tools described in the following sections:

- Cisco Feature Navigator, page 565
- Cisco IOS Documentation Set, page 565

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is available 24 hours a day, 7 days a week, and is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/

Cisco IOS Documentation Set

The Cisco IOS documentation set includes configuration guides, command references, release notes, system message guides, and master command lists. For all new and revised Cisco IOS documentation for the Cisco IOS 15.2M&T releases, see the following URL:


Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).
License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:
Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:
Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.
This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, Ihash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

   The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.