# Release Notes for Cisco IOS Release 15.3M&T

**First Published: November 29, 2012**

**Last Updated: July 19, 2013**

**Release: Cisco IOS Release 15.3(3)M**

**Part Number: OL-28172-04**

These release notes support Cisco IOS Release 15.3M&T up to and including Cisco IOS Release 15.3(3)M. The release notes are updated with each 15.3M&T release to describe new features and related documents.

Cisco IOS Release 15.3M&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

# Cross-Platform System Requirements

This section describes the system requirements for Cisco IOS Release 15.3M&T and includes the following sections:



## Supported Hardware Platforms

Cisco IOS Release 15.3M&T supports platforms within the following Cisco series:

- Cisco 800 series routers
- Cisco 1900 series integrated services routers
- Cisco 2900 series integrated services routers
- Cisco 3900 series integrated services routers
- Cisco Connected Grid Router (CGR) 2000 series (CGR 2010)
- Cisco Analog Voice Gateways (VG202XM and VG204XM)
- Cisco High Density Analog Voice Gateways (VG350)

For more information about the platforms supported in Cisco IOS Release 15.3M&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 IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.3(3) M, 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:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml

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

http://www.cisco.com/en/US/prod/iosswrel/networking_solutions_products_genericcontent0900aecd806ea5be.html

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

- Cisco 800 series routers:

  http://www.cisco.com/en/US/products/hw/routers/ps380/prod_installation_guides_list.html

- Cisco 1900 series routers:

  http://www.cisco.com/en/US/docs/routers/access/1900/hardware/installation/guide/1900_HIG.html

- Cisco 2900 and 3900 series routers:

  http://www.cisco.com/en/US/docs/routers/access/2900/hardware/installation/guide/Hardware_Installation_Guide.html

- Cisco Connected Grid Routers 2010:

  http://www.cisco.com/en/US/products/ps10977/prod_installation_guides_list.html

- Cisco VG202XM and Cisco VG204XM Voice Gateways:

  http://www.cisco.com/en/US/docs/routers/access/vg202_vg204/hardware/vg2_vg4hw.html

- Cisco VG350 Voice Gateway:

  http://www.cisco.com/en/US/docs/routers/access/vg350/hardware/installation/guide/vg350_hig.html

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

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

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://tools.cisco.com/ITDIT/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:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

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:

http://tools.cisco.com/RPF/register/register.do

# 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 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 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 or Technology Selection Page

  http://www.cisco.com/cisco/web/psa/troubleshoot.html?mode=prod&level0=268437899
- *Cisco 800 Series Routers Troubleshooting Guides*

  http://www.cisco.com/en/US/products/hw/routers/ps380/prod_troubleshooting_guides_list.html
- *Cisco 1600 Series Routers Hardware Troubleshooting Index Page*

  http://www.cisco.com/en/US/products/hw/routers/ps214/products_tech_note09186a008012fb88.shtml
- *Troubleshooting Cisco 3900 Series, 2900 Series, and 1900 Series ISRs*

  http://www.cisco.com/en/US/docs/routers/access/2900/hardware/installation/guide/Trouble.html
- *Cisco Unified Communications 500 Series Install and Upgrade Tech Notes*

  http://www.cisco.com/en/US/products/ps7293/tsd_products_support_install_and_upgrade_technotes_list.html
- *Cisco Error Message Decoder*

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
- 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:

http://www.cisco.com/web/applicat/CFNTOOLS/Help_Docs/help/cfn_support.html

## 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.

**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.

**Step 7** 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 15.3M&T supports the following Cisco series:

# Cisco 800 Series Routers

Cisco IOS Release 15.3M&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 881, Cisco 881G, Cisco 881GW, Cisco 881SRST, Cisco 881W, Cisco 881WD, Cisco 881-CUBE
- Cisco 886VA, Cisco 886VAG, Cisco 886VA-W, Cisco 886-CUBE
- 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 892FSP, Cisco 892F-CUBE
- Cisco 898EA

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

http://www.cisco.com/en/US/products/hw/routers/ps380/index.html

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 15.3M&T are also available through Cisco Feature Navigator.

# Cisco 1900 Series Integrated Services Routers

Cisco IOS Release 15.3M&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:

http://www.cisco.com/en/US/products/ps10538/index.html

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 15.3M&T are also available through Cisco Feature Navigator.

# Cisco 2900 Series Integrated Services Routers

Cisco IOS Release 15.3M&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:

http://www.cisco.com/en/US/products/ps10537/index.html

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 15.3M&T are also available through Cisco Feature Navigator.

# Cisco 3900 Series Integrated Services Routers

Cisco IOS Release 15.3M&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:

http://www.cisco.com/en/US/products/ps10536/index.html

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 15.3M&T are also available through Cisco Feature Navigator.

# Cisco Connected Grid Router 2000 Series

Cisco IOS Release 15.3M&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:

http://www.cisco.com/en/US/products/ps10977/index.html

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 15.3M&T are also available through Cisco Feature Navigator.

# Cisco Analog Voice Gateways

Cisco IOS Release 15.3M&T supports the following analog voice gateways:

- Cisco VG202XM
- Cisco VG204XM

For detailed information about Cisco analog voice gateways, see the documents at the following location:

http://www.cisco.com/en/US/products/hw/gatecont/ps2250/index.html

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 15.3M&T are also available through Cisco Feature Navigator.

# Cisco High Density Analog Voice Gateways

Cisco IOS Release 15.3M&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:

http://www.cisco.com/en/US/products/hw/gatecont/ps2250/index.html

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 15.3M&T are also available through Cisco Feature Navigator.

# Features and Important Notes for Cisco IOS Release 15.3(3)M

These release notes describe the following topics:



## New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.3(3)M and contains the following subsections:



### New Hardware Features Supported in Cisco IOS Release 15.3(3)M

This section describes new and changed features in Cisco IOS Release 15.3(3)M. Some features may be new to Cisco IOS Release 15.3(3)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 15.3(3)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.

#### EtherSwitch Service Module

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

Need URL or RN-only blurb (FTS-13660-1; mnapalan)

### New Software Features Supported in Cisco IOS Release 15.3(3)M

This section describes new and changed features in Cisco IOS Release 15.3(3)M. Some features may be new to Cisco IOS Release 15.3(3)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 15.3(3)M. Links to feature modules are included. If a feature listed does not have a link to a feature module, that feature is documented only in the release notes.

#### BFD Multihop Support for IPv4 Static Routes

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-mt/irb-15-mt-book_chapter_0111.html

#### BGP- Local-AS Allow-Policy

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

http://www.cisco.com/en/US/partner/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-local-as-policy-1.html

### BGP - RT / VPN-ID Attribute Rewrite Wildcard

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-vpn-distinguisher-range1.html

### BGP - VRF Aware Conditional Advertisement

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-vrf-conditional-adv.html

### Browser Based Auth Bypass (JLL)

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_auth/configuration/15-mt/sec-brwsr-auth-bypass.html

### Cisco Unified Communications Manager Express 10.0

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

### CUBE as a Flow Metadata Producer

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_mgmt/configuration/15-mt/voi-cube-flow-metadata.html

### CUBE Inter-Cluster Look up Service (ILS)

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_interop/configuration/15-mt/voi-cube-ils-service.html

### CUBE Serviceability for Event Logging and Debug Classification

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_mgmt/configuration/15-mt/voi-cube-service-evntlog-debugclass.html

### CUCM Lineside Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_mgmt/configuration/15-mt/voi-cucm-lineside.html

### Default User-Group support for Authentication

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/scansafe-web-sec.html

### Firmware Upgrade For G.SHDSL

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

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_ATM_HWICS.html

### GETVPN CRL Checking

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-mt/sec-get-vpn-crl-checking.html

### GETVPN Resiliency - GM Error Detection

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-mt/sec-get-vpn-resiliency-gm-error-detection.html

### IP SLAs - Asymmetric Probe Support for UDP Jitter

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-mt/sla_udp_jitter.html

### IPv6: RIPng VRF Aware Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_rip/configuration/15-mt/irr-ipv6-ripng.html

### IPv6 SNMP MIB Support For Voice Features

The MIB objects relevant to Cisco UBE that have transport-related information such as IPV6 address and type of IP (IPV4 or IPV6) have been verified. The criteria used for the enhanced MIBs are:

- The MIB should have voice/video related information.
- MIB objects should have IP address element in them.

The following MIBs satisfied the above criteria:

- CISCO-VOICE-DIAL-CONTROL-MIB
- CISCO-RTTMON-MIB
- CISCO-RTTMON-IP-EXT-MIB
- CISCO-SIP-CALLS-MIB
- CISCO-POP-MGMT-MIB

### IS-IS - Inbound Filtering

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-mt/isis-inbound-filtering.html

### ISR-G2 Licensing Modifications

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

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

### MIBs, SMS, GPS, Multiple Profile

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

Need URL or RN-only blurb (FTS-13811-1; dmcalpin)

### NanoCube

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/nanocube/configuration/15-mt/nanocube-config-15-mt-book.html

### Network-based Recording of Video Calls Using Cisco UBE

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/15-mt/voi-ntwk-based-rec-video-calls.html

### Nested LDAP Group Search for Microsoft AD

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ldap/configuration/15-mt/sec_nested_ldap.html

### Object Tracking: IPv6 Route Tracking

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/15-mt/iap-ipv6-route-track.html

### onePK Enhancements

onePK is an easy-to-use toolkit that enables software developers to access, extend, or customize the rich set of software functionality provided by Cisco routers and switches.

### PKI - New Cert Attributes

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

http://www.cisco.com/en/US/docs/ios/15_3m_and_t/release/notes/drafts/15_3m_feats_important_notes.html

### Recursive Static Route

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/configuration/15-mt/iri-recursive-static-route.html

### Scansafe Tower Telemetry

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/scansafe-web-sec.html

### SSH-Ability to Disable Autentication Methods

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/15-mt/sec-ssh-config-auth.html

### TDOS Attack Prevention on CUBE

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/15-mt/voi-cube-tdos-attack-mitigation.html

### UC GW Services - Media Forking Service

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/15-mt/voi-cube-uc-gateway-services.html

### Video Quality Metrics

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

http://www.cisco.com/en/US/docs/routers/access/spectacles/configuration/guide/VQM_guide.html

### Voice Quality Monitoring

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/nanocube/configuration/15-mt/voi-nanocube-voice-quality-monitoring.html

### VRF Awareness for TCP Raw Sockets

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

http://www.cisco.com/en/US/docs/routers/connectedgrid/cgr2010/software/15_2_4_m/raw_socket.html

### VRRPv3: Object Tracking Integration

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/15-m/fhrp-vrrpv3-obj-trk.html

# MIBs

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

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

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

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access the 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:

http://tools.cisco.com/RPF/register/register.do

# Important Notes

The following sections contain important notes about Cisco IOS Release 15.3M:

- Field Notices and Bulletins, page 20

## Field Notices and Bulletins

- Field Notices—Cisco recommends 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.
- Bulletins—You can find bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_literature.html.

# Features and Important Notes for Cisco IOS Release 15.3(2)T

## Contents



## New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.3M&T and contains the following subsections:



**Note** A cumulative list of all new and existing features supported in a 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 15.3(2)T

This section describes new and changed features in Cisco IOS Release 15.3(2)T. Some features may be new to Cisco IOS Release 5.3(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 15.3(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.


**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

### EHWIC-4SHDSL-EA

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

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_ATM_HWICS.html

### VG202XM, VG204XM

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

http://www.cisco.com/en/US/docs/routers/access/vg202_vg204/hardware/vg2_vg4hw.html

## New Software Features Supported in Cisco IOS Release 15.3(2)T

This section describes new and changed features in Cisco IOS Release 15.3(2)T. Some features may be new to Cisco IOS Release 15.3(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 15.3(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.

### Add Path Support in EIGRP

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-mt/ire-add-path-15mt.html

### BFD for RIPv2 Support

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

http://www.cisco.com/en/US/docs/ios/iproute_rip/configuration/guide/irr_bfd_ripv2.html

### BFD Single Hop Authentication

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15MT/irb-bfd-shop-auth.html

### BGP—Multicast VPN BGP Dampening

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-mvpn-damp.html

## BGP—Multi-Cluster ID

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-multicluster-id.html

## BGP—VPN Distinguisher Attribute

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-vpn-distinguisher.html

## BowFlex—IKEv2

The Bowflex—IKEv2 feature enhances Cisco software by improving the quality of the crypto component code by upgrading the existing Internet Key Exchange (IKE) and Internet Key Exchange Version 2 (IKEv2) hardening features through the following commands:

- **clear crypto ikev2 stats**—Clears IKEv2 SA statistics.
- **debug crypto isakmp**—Displays messages about IKE events.
- **show crypto ikev2 stats**—Displays IKEv2 SA statistics.
- **show crypto isakmp diagnose error**—Displays IKE error diagnostics.

For more information on the above commands, refer to the following documents:

Cisco IOS Security Command Reference: Commands S to Z

http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html

Cisco IOS Debug Command Reference: Commands I through L

http://www.cisco.com/en/US/docs/ios-xml/ios/debug/command/a1/db-a1-cr-book.html

## Bowflex—ISM VPN Reventon Debug Enhancement

The Bowflex—ISM VPN Reventon Debug Enhancement feature enhances the functionality of the existing Cisco VPN Internal Service Module (ISM) data path implementation by improving debugging capacity in Reventon. This feature does not include any architectural changes to the existing Reventon hardware or software but only implements the intended functionality on top of the existing architecture through the following commands:

- **debug crypto engine ism-vpn**—Enables debugging for Cisco VPN ISM.
- **debug crypto engine ism-vpn traffic**—Enables debugging for a Cisco VPN ISM traffic.
- **debug crypto engine ism-vpn traffic selector**—Enables debugging for selective traffic in Cisco VPN ISM.
- **debug crypto engine ism-vpn ssl**—Enables debugging for Secure Socket Layer (SSL) in Cisco VPN ISM.
- **show crypto engine accelerator statistic**—Displays IPsec encryption statistics and error counters for the onboard hardware accelerator of a device, the IPsec VPN SPA, or the Cisco VPN ISM.

For more information on the above commands, refer to the following documents:

Cisco IOS Debug Command Reference: Commands A through D

http://www.cisco.com/en/US/docs/ios-xml/ios/debug/command/a1/db-a1-cr-book.html

Cisco IOS Security Command Reference: Commands S to Z

http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html

## Bowflex—NHRP Hardening and Debug Enhancement

The Bowflex—NHRP Hardening and Debug Enhancement feature enhances the quality of the crypto component code by upgrading the NHRP hardening in Internet Key Exchange (IKE) by adding the following commands:

- **debug nhrp (IKE)**—Displays detailed information about the NHRP debugging information.
- **clear ip nhrp**—Clears dynamic entries from the NHRP cache.
- **show ip nhrp traffic**—Displays NHRP traffic statistics.
- **show ip nhrp multicast**—Displays NHRP multicast mapping.

For more information on the above commands, refer to the following documents:

Cisco IOS IP Addressing Services Command Reference

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-cr-book.html

Cisco IOS Debug Command Reference: Commands M through R

http://www.cisco.com/en/US/docs/ios-xml/ios/debug/command/m1/db-m1-cr-book.html

## Call Progress Analysis (CPA) over IP-IP Media Session

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/15-mt/voi-cube-cpa.html

## Cisco TrustSec with SXPv4

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_cts/configuration/15-mt/sec-cts-sxpv4.html

## Cisco Unified Communications Manager Express 9.5

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html

## CUBE Support for IPv6

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/15-mt/voi-voip-ipv6.html

## Diagnostic Signatures

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ha/configuration/15-mt/ha-config-diag-sign.html

## EVN Cisco EVN MIB

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

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-mgt-ts.html

## EVN EIGRP

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

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-confg.html

## EVN Multicast

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

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-confg.html

## EVN OSPF

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

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-confg.html

## EVN Route Replication

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

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-shared-svcs.html

## EVN Traceroute

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

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-mgt-ts.html

## EVN VNET Trunk

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

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-confg.html

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-mgt-ts.html

http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-mt/evn-overview.html

## GET VPN Hardening

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-mt/sec-get-vpn.html

## GET VPN Resiliency

This feature improves the resiliency of the Cisco Group Encrypted Transport VPN technology, so that data traffic disruption is prevented or minimized when errors occur.

This feature introduces long security association (SA) lifetime functionality, which extends the maximum for which you can configure the lifetime of the key encryption key and traffic encryption keys from 24 hours to 30 days. This feature also lets you configure key servers to continue to send periodic reminder rekeys to group members that do not respond with an acknowledgment in the last scheduled rekey.

By using a long SA lifetime in combination with periodic reminder rekeys, a key server can effectively synchronize group members if they miss a scheduled rekey before the keys roll over.

The following commands are modified for this feature:

- The **rekey lifetime** command was modified. The **days** *days* keyword and argument pair was added, and the range of values for the **seconds** *seconds* keyword and argument pair was extended.
- The **rekey retransmit** command was modified. The **periodic** keyword was added.
- The **set security-association lifetime** command was modified. The **days** *days* keyword and argument pair was added, and the range of values for the **seconds** *seconds* keyword and argument pair was extended.
- The **show crypto gdoi** command was modified. Output was added to show the time until the next rekey.
- The **show crypto gdoi feature** command was modified. The **long-sa-lifetime** keyword was added, which displays the version of the GET VPN software running on each key server and group member in the GET VPN network and displays whether each of those devices is running a version that supports a long SA lifetime.
- The **show crypto gdoi gm replay** command was modified. Output was added to show information about the last 50 time-based antireplay errors.
- The **show crypto gdoi ks rekey** command was modified. Output was added to show the number of rekey retransmissions, the current retransmit period, and the time until the next retransmission.
- The **show crypto gdoi ks policy** command was modified. Output was added to show the time until the next rekey.

## GET VPN Support of IPsec Inline Tagging for Cisco TrustSec

Cisco TrustSec (CTS) uses the user and device identification information acquired during authentication to classify packets as they enter the network. CTS maintains classification of each packet by tagging packets with security group tags (SGTs) on ingress to the CTS network so that they can be identified for applying security and other policy criteria along the data path. The tags allow network intermediaries

such as switches and firewalls to enforce the access control policy based on the classification. The GET VPN Support of IPsec Inline Tagging for Cisco TrustSec feature uses GET VPN inline tagging to carry the SGT information across the private WAN.

The following commands are new or modified for this feature:

- The **show crypto gdoi feature** command was modified. The **cts-sgt** keyword was added, which displays the version of the GET VPN software running on each key server and group member in the GET VPN network and displays whether each of those devices is running a version that supports the GET VPN Support of IPsec Inline Tagging for Cisco TrustSec feature.
- The **show crypto ipsec sa detail** command was modified. Output was added to display the number of packets tagged with an SGT (in the outbound direction) and the number of packets not tagged with an SGT (in the inbound direction).
- The **tag cts sgt** command was introduced. This command enables CTS SGT inline tagging in a GDOI group IPsec security association.

## Graceful Shutdown Support for OSPFv3

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-15-mt-book.html

## HSRP—Global IPv6 Address

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/ip6-fhrp-hsrp.html

## IEC 60870-5-101/104 SCADA Gateway

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

http://www.cisco.com/en/US/products/ps10977/products_installation_and_configuration_guides_list.html

## IP SLA—Percentile Support for Filtering Outliers

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-mt/sla_any-percent.html

## IPv6 Support for LDAP

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ldap/configuration/15-mt/sec_ipv6_ldap.html

## ISIS No Hello Padding Always

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/command/irs-cr-book.html

## NAT Box-to-Box HA Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/iadnat-b2b-ha.html

## OSPFv3 ABR Type 3 LSA Filtering

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-abr-type-3.html

## PfR SNMP Traps v1.0

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

http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-mt/pfr-snmp-trap.html

## Prefix Suppression Support for OSPFv3

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-15-mt-book.html

## QoS—Queue-Limit and WRED Enhancements

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos/command/Q_through_R.html
#GUID-D82A59DD-D709-4C51-8DF2-26C29C21DA01

## Simple Network Time Protocol V4 (SNTPV4)

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

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-mt/bsm-sntpv4.html

## Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-SIP Call on the Cisco Unified Border Element

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/15-mt/
voi-negt-aud-code.html

## TDM-SIP GW for IPv6

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cminterop/configuration/15-mt/voi-ip6-voip.html

### WEBEX Telepresence Media Support over Single SIP Session

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_proto/configuration/15-mt/voi-webex-telepresence.html

# Important Notes

The following information applies to all releases of Cisco IOS Release 15.3M&T.

- Field Notices and Software-Related Tools and Information, page 29

## 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 Download Software page at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm.

# Features and Important Notes for Cisco IOS Release 15.3(1)T

## Contents



## New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.3M&T and contains the following subsections:



**Note** A cumulative list of all new and existing features supported in a 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 15.3(1)T

This section describes new and changed features in Cisco IOS Release 15.3(1)T. Some features may be new to Cisco IOS Release 15.3(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 15.3(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.


**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

### High Density FXS Module Support on Cisco ISR G2

The High Density FXS Module Support on Cisco ISR G2 feature provides High Density FXS module support for the Cisco ISR G2.

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

http://www.cisco.com/en/US/docs/routers/access/vg350/hardware/installation/guide/vg350_hig.html

## New Software Features Supported in Cisco IOS Release 15.3(1)T

This section describes new and changed features in Cisco IOS Release 15.3(1)T. Some features may be new to Cisco IOS Release 15.3(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 15.3(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.

### AutoInstall Support for TCL Script

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ios_tcl/configuration/15-mt/ios-tcl-15-mt-book.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ios_tcl/configuration/15-mt/nm-autoinstall-script-tcl.html

### BGP—Add Path

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-additional-paths.html

### BGP—Attribute Filter and Enhanced Attribute Error Handling

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-attribute-filter.html

### BGP—mVPN SAFI-129 IPv6

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-mvpn-safi-ipv6.html

### BGP Support for IP Prefix Export from a VRF Table into the Global Table

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-mt/irg-prefix-export.html

## Cisco Data Collection Manager

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

http://www.cisco.com/en/US/docs/ios-xml/ios/bsdcm/configuration/15-mt/bsdcm-15-mt-book.html

http://www.cisco.com/en/US/docs/ios-xml/ios/bsdcm/configuration/15-mt/nm-bs-dcm.html

## CUBE Serviceability

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_mgmt/configuration/15-mt/voi-cube-serviceability.html

## Cisco VG350 No Payload Encryption (NPE) Image

The Cisco VG350 No Payload Encryption (NPE) Image feature provides a Cisco IOS image for the Cisco VG350 without payload encryption (NPE).

## Diffserv MIB

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_dfsrv/configuration/15-mt/qos-dfsrv-mib.html

## EIGRP IPv6 MIBs

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2mt/ire-mib.html

## Flexible NetFlow—Classification/MQC Integration

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

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/guide/15-mt/fnf-fnf-mqc.html

## Flexible NetFlow—IPFIX Export Format

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

http://www.cisco.com/en/US/docs/ios-xml/ios/media_monitoring/configuration/15-2mt/mm-pasv-mon.html

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-mt/cfg-de-fnflow-exprts.html

http://www.cisco.com/en/US/docs/ios-xml/ios/avc/configuration/15-mt/cfg-avc-mace.html

## Flow Metadata IPv6 Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mdata/command/mdata-cr-book.html

## HSRP-Aware PIM

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-mt/imc_hsrp_aware.html

## IP SLA—OnDemand UDP Probes

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-mt/sla_udp_ondemand.html

## ISIS BFD TLV

The IS-IS Bidirectional Forwarding Detection (BFD) Tag Length Value (TLV) feature provides a faster method to detect a loss of an IS-IS adjacency. Before, when an IS-IS adjacency reached the UP state (and therefore could be used for forwarding), a BFD session needed to be established with that neighbor. Now, a BFD session is maintained as long as the hello holddown timer for the neighbor does not expire, which is new for BFD TLV. The BFD session is only deleted if the neighbor hello times out. If BFD signals to IS-IS that a session has gone DOWN, the adjacency associated with that session will transition to DOWN state. Once the BFD session goes back UP, the adjacency state can transition back to an UP state.

For a given IS-IS topology, IS-IS determines if BFD is usable for a given neighbor on that topology. BFD is not usable when BFD is enabled on both sides and the BFD session is down. When there are multiple BFD sessions enabled for different address families, such as IPv4 and IPv6, if BFD is not usable for any address family, then BFD is consider not usable for the entire adjacency on that topology. For example, if both IPv4 and IPv6 BFD are enabled for single topology, if either the IPv4 BFD session is down or IPv6 BFD session is down, the neighbor state will be set to DOWN state. If BFD is not enabled for a given address family, then BFD is considered usable for that address family.

For single topology mode, the neighbor state is down when either the IPv4 or IPv6 BFD session is not BFD usable, that is, if BFD is enabled on both sides and the BFD session is DOWN. If BFD is not enabled on either side, BFD will be set to TRUE. For multi-topology mode, IS-IS adjacency will be in UP state as long as any topology is UP . However, the neighbor for the topology where BFD is consider not usable is considered down for that specific topology. For example, if both IPv4 and IPv6 BFD are enabled, and the IPv4 session is DOWN and IPv6 session is UP, then the IS-IS adjacency is still UP. In this case, the IPv4 neighbor is considered DOWN and ipv6 neighbor is considered UP.

## ISIS Client for BFD C-Bit Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-mt/irb-bfd-isis-cbit.html

## ISIS IPv6 Client for BFD

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-mt/ip6-bfd-isis-client.html

## LISP Delegate Database Tree (DDT)

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_lisp/configuration/15-mt/irl-ddt.html

## LISP Host Mobility Across Subnet

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_lisp/configuration/15-mt/irl-host-mob.html

## LISP Security (LISP-Sec)

The LISP Security (LISP-Sec) feature enables a set of security mechanisms that provide origin authentication, integrity, and anti-replay protection for map-request/map-reply mapping resolution exchanges.

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_lisp/command/ip-lisp-cr-book.html

## MACE Phase-2 Enhancements

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

http://www.cisco.com/en/US/docs/ios-xml/ios/avc/configuration/15-mt/cfg-avc-mace.html

## MediaTrace 3.0 —MIB, IPv6, MIB Profiles, and Reverse MediaTrace

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

http://www.cisco.com/en/US/docs/ios-xml/ios/media_monitoring/configuration/15-mt/mm-mediatrace.html

## Metadata Spectacle Integration Phase-1

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mdata/configuration/15-mt/metadata-framework.html

## MVPNv6

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_mvpn/configuration/15-mt/imc_mvpnv6.html

## NAT TCP SIP ALG Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html

## NBAR2 Custom Protocol

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/configuration/15-mt/nbar2-custom-protocl.html

## NETCONF XML PI

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

http://www.cisco.com/en/US/docs/ios-xml/ios/cns/configuration/15-mt/cns-netconf.html

## OSPFv3 Retransmission Limits

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-15-mt-book.html

## OSPFv3 RFC 3101 Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-cfg.html

## PfR Bandwidth Visibility Distribution for xDSL Access

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

http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-mt/pfr-band-vis.html

## PIM Allow RP

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-mt/imc_pim_allowrp.html

## Protocol Pack Licensing

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/configuration/15-mt/NBAR_Protocol_Pack.html

## Shaping on Dialer Interface

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_conavd/configuration/15-mt/qos-conavd-dial.html

## TTL Security Support for OSPF on IPv6

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-ttl-sec-ospfv3.html

# Important Notes

The following information applies to all releases of Cisco IOS Release 15.3M&T.



## 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 15.3(1)T1

The following behavior changes are introduced in Cisco IOS Release 15.3(1)T1:

- 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:
  http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html

- Position of MP_REACH Attribute in Attributes List of BGP Updates

  Old Behavior: If the BGP Enhanced Attribute Error Handling feature is enabled, BGP places the MP_REACH attribute (attribute 14) at the beginning of the attributes list while formatting an update. If the feature is not enabled, BGP places the MP_REACH attribute at the end of the attributes list, which makes handling a malformed update more difficult for neighbor routers that are doing enhanced error handling.

  New Behavior: Whether or not the BGP Enhanced Attribute Error Handling feature is enabled, BGP places the MP_REACH attribute (attribute 14) at the beginning of the attributes list while formatting an update. Enhanced error handling can function much more easily when the MP_REACH attribute is at the beginning of the attributes list.

- 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:
  http://www.cisco.com/en/US/docs/ios/wan/command/reference/wan_s2.html#wp1101997

# 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 Download Software page at http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm.

# Caveats for Cisco IOS Release 15.3(3)M

## 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.

**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. (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:


- Open Caveats—Cisco IOS Release 15.3(3)M, page 39
- Resolved Caveats—Cisco IOS Release 15.3(3)M, page 41


## Open Caveats—Cisco IOS Release 15.3(3)M

All the caveats listed in this section are open in Cisco IOS Release 15.3(3)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCuh56073

  Symptom: Cellular interface is not able to retrieve the IP address of an established call. Modem and host are out of sync (Stale IP).


**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Conditions: This symptom occurs when the cellular interface fails to get the SP assigned IP address from the modem when the cellular call is up. A router reload may be required.

Workaround: If you are using C819G-4G-V-K9, DO NOT use any image from Cisco IOS Release 15.3(3)M. Instead, in the interim, use an image from Cisco IOS Release 15.2(4)M3.

- CSCuh78663

  Symptom: Host system loses connectivity with modem.

  Conditions: This symptom is observed when, after modem power-cycles, Cisco router fails to initialize the USB connection to modem and keep resetting the modem. A router reload may be required.

  Workaround: If you are using C819G-4G-V-K9 or EHWIC-4G-LTE-V, DO NOT use any image from Cisco IOS Release 15.3(3)M. Instead, in the interim, use an image from Cisco IOS Release 15.2(4)M3.

- CSCuh67111

  Symptom: Modem and SDK loses connection.

  Conditions: This symptom is observed when the network connection (data bearer) to the SP is reset multiple times in very short duration (multiple resets per minute), the router cellular interface becomes non-responsive and goes in hang state. The SDK driving the modem crashes. A router reload may be required.

  Workaround: If you are using C819G-4G-V-K9, DO NOT use any image from Cisco IOS Release 15.3(3)M. Instead, in the interim, use an image from Cisco IOS Release 15.2(4)M3.

- CSCuh81523

  Symptom: Modem is in potential hang state.

  Conditions: This symptom is observed when the IOS gets irregular parameter value with new SDK leading to link recovery. This results in cellular interface resets.

  Workaround: If you are using C819G-4G-V-K9 or EHWIC-4G-LTE-V, DO NOT use any image from Cisco IOS Release 15.3(3)M. Instead, in the interim, use an image from Cisco IOS Release 15.2(4)M3.

- CSCug55040

  Symptoms: The cellular interface stops sending or receiving traffic due to modem crash.

  Conditions: This symptom is observed when bi-directional iMIX traffic is sent from test center with 5 Mbps Uplink and 12 Mbps Downlink. Traffic is sent normally for about an hour, then the modem/IOS get heart beat timeout and traffic stop sending.

  Workaround: Modem power cycle (link recovery). There may be two to three minutes loss of connectivity.

- CSCug22606

  Symptoms: The cellular interface become non-responsive due to SDK crash.

  Conditions: This symptom is observed when the network connection (data bearer) to the SP is reset multiple times in very short duration (multiple resets per minute), the router cellular interface becomes non-responsive and hangs causing the SDK driving the modem to crash. A router reload is required to recover from it.

  Workaround: Modify the “embedded link recovery monitor-time” parameter from 20 seconds to 60 seconds.

# Resolved Caveats—Cisco IOS Release 15.3(3)M

The caveats in this section are resolved in Cisco IOS Release 15.3(3)M but may be open in previous Cisco IOS releases.

- CSCti87912

  Symptom: While bringing up PPP sessions, server fails to add a route to the client after the IPCP negotiation.

  Conditions: This symptom occurs with the following two conditions:

  1. "ip unnumbered..." per user configuration that is received from radius is applied on the virtual-access interface.
  2. Virtual-template used for virtual-access creation is configured with "ip unnumbered <>".

  Workaround: There is no workaround.

- CSCto03904

  Symptom: DSP is restarted when PCMU is transcoded to iLBC on DSP-SPA after **rtcp-regenerate** is enabled.

  Conditions: This symptom occurs when PCMU is transcoded to iLBC on DSP-SPA after **rtcp-regenerate** is enabled.

  Workaround: Do not enable **rtcp-regenerate**.

- CSCtq02528

  Symptom: A Cisco router crashes when executing **show ip ips session**.

  Conditions: This symptom is observed when you have the IPS configured and applied to at least one interface.

  Workaround: Disable the IPS configuration.

- CSCtr19078

  Symptom: An IO memory leak in a Cisco router occurs with the following error message:

  ```
  SYS-2-MALLOCFAIL: Memory allocation of x bytes failed Pool: IO Alternate Pool: None
  Free: 0 Cause: No Alternate Pool
  ```

  Conditions: This symptom is observed in a Cisco 3270 router with QoS enabled. When IPSEC encryption is configured on an SVI (3270 FESMIC Port) using the QoS pre-classify option, the router's memory is quickly exhausted. This happens because traffic routed out of this interface is encrypted but when the same traffic with pre-classify enabled is directed through the native Layer 3 port (MARC card ports), the Cisco 3270 router works fine.

  Workaround: Disable QoS pre-classify using the **no qos pre- classify** command.

- CSCts86510

  Symptom: Unable to build dIOU images.

  Conditions: This symptom is observed while compiling unused dIOU images.

  Workaround: There is no workaround.

- CSCtu08717

  Symptom: A Cisco router experiences a watchdog timeout while executing **tw_timer_replenish**.

  Conditions: This symptom is observed on the Cisco router if the IP SLA and Performance Agent features are configured on it. This timeout may also be observed if traffic is sent for a long time through a Cisco router configured with these features.

Workaround: There is no workaround.

- CSCtu21636

  Symptom: Sometime calls are dropped if there are active calls on the DSP. The following errors are displayed in the logs:

  ```
  Power alarm on DSP channel ch=1 is ON 0001 0001 **
  Power alarm on DSP channel ch=1 is OFF 0001 0000 **
  Power alarm on DSP channel ch=1 is ON 0001 0001 **
  Power alarm on DSP channel ch=1 is OFF 0001 0000 **
  ```

  Conditions: This symptom is seen with all conditions.

  Workaround: There is no workaround.

- CSCty26575

  Symptom: After reload, the following error message is displayed:

  ```
  *TTY0: timer_create_bg error*
  ```

  Conditions: This symptom occurs under the following conditions:

  - When the following CLI, ***exec-timeout 30 0***, is configured in line console 0
  - When the router is reloaded.

  Workaround: There is no workaround.

- CSCtz84873

  Symptom: A crash is observed due to stack overflow:

  ```
  %SYS-6-STACKLOW: Stack for process CCSIP_SPI_CONTROL running low, 0/60000
  ```

  Conditions: The issue is seen on a SIP gateway.

  Workaround: There is no workaround.

- CSCub33602

  Symptom: IGMP query, with source IP address: 0.0.0.0, triggers a querier election process. As a consequence, port on which this packet is received is marked as mrouter port for that VLAN.

  ```
  Router#show ip igmp int vlan 1 Vlan1 is up, line protocol is up Internet address is
  1.1.1.1/24 IGMP querying router is 0.0.0.0 <----
  Router#sh ip igmp snooping mrouter vlan ports
  -----+---------------------------------------- 1 Po1,Po8,Router<-----
  ```

  Conditions: This symptom is seen when IGMP query with source IP address: 0.0.0.0 is received.

  Workaround: Configure an ACL to block packets with source IP address: 0.0.0.0 and apply it to relevant interfaces.

  ```
  access-list 100 deny ip host 0.0.0.0 any access-list 100 permit ip any any int vlan 1
  ip access-group 100 in
  ```

  Further Problem Description: Per RFC 4541, IGMP query with source IP address: 0.0.0.0 is used in special cases. When such query is received by a router, it should not be used in the querier election process.

- CSCub34396

  Symptom: Due to the fix for CSCtw52819, non-NHRP process switched packets and are noticed to go as clear text.

  Conditions: This symptom is observed with a DMVPN configuration.

Workaround: There is no workaround.

- CSCub36684

  Symptom: Slow memory leak is observed.

  Conditions: This symptom occurs due to the SNMP engine.

  Workaround: There is no workaround.

- CSCuc83061

  Symptom: In a SAF setup with EIGRP, the EIGRP peers are seen flapping continuously when there are mixed TLV version neighbors on a single interface.

  Conditions: This symptom occurs when EIGRP Service-family neighbor-ship flaps are seen at random intervals. There is no definite pattern to these flaps, and they are not restricted to any one peer in the network. This issue is seen when there are two different TLV versions and they are on the same interface, and if service data is greater than 8KB.

  Workaround: There is no workaround. If one of the mixed peers is removed from the interface, the issue will not be seen.

- CSCue17104

  Symptom: When multipath static routes are added and if they exceed the maximum multipath route limit for the platform, the routes will not be installed in the RIB. Later, when installed routes are unreachable, the previously uninstalled routes are not added back.

  Conditions: This symptom is observed with multipath static routes. The maximum number of multipath routes for a destination depends on the platform. For instance, it is eight for Cisco Catalyst 4500 Series.

  Workaround: Issue the following command:

  **clear ip route <route>**

- CSCue41011

  Symptom: BFD sessions not coming up after shut/no shut. To recreate the issue:

  1. Create 510 BDI interfaces on both rudys such that 255 are on one physical interface.
  2. Map all the BDI interfaces to corresponding 255 VRF's.
  3. Enable any routing protocol for each VRF & BFD on all the BDI's.
  4. Perform interface shut/no-shut.

  Conditions: This symptom is observed when discriminator is exhausted. Release the discriminators if the sessions are in inactive queue.

  Workaround: Bring down the sessions and then bring them up again.

- CSCue48419

  Symptom: The Cisco AS5350 Universal Gateway stops processing calls on PRI with a signaling backhaul from PGW. In the packet trace, there is no q931message from PGW. Further analysis shows that Cisco AS5350 Universal Gateway sends a q_hold (0x5)message in BSM, causing peer (PGW) to stop sending signaling traffic. However, there is no BSM_resume message or BSM_reset sent after it. Hence, PGW is stuck in this condition. There was an earlier defect for CSCts75818 with similar symptoms in U-state.

  Conditions: This symptom is observed due to some RUDP timing issues that causes BSM session switchover.

  Workaround: Reload the Cisco AS5350 Universal Gateway (but only when CU notices the outage). Also, shutting both Ethernet interfaces may help, but this workaround has not been tested.

- CSCue60618

  Symptom: The ability to shut NMSP (default) service on TCP port 16113.

  Conditions: This symptom is observed in the default configuration.

  Workaround: There is no workaround.

  More Info: After this fix, the NMSP feature needs to be explicitly enabled using CLI **nmsp enable**. This change satisfies the security baseline requirement that no TCP ports should be open as a default option. The NMSP port 16113 can now be disabled with CLI **no nmsp enable** which was not an option before this fix.

- CSCue89779

  Symptom: A FlexVPN spoke configured with an inside VRF and front-door VRF may have problems with spoke-to-spoke tunnels if they are not same. During tunnel negotiation, two Virtual-access interfaces are created (while only one is needed), the one in excess may fail to cleanup correctly. As a result, the routes created by NHRP process may lead to loss of traffic, or traffic may continue to flow through the Hub.

  Conditions: This symptom occurs when the VRF used on the overlay (IVRF) and the VRF used on the transport (FVRF) are not same.

  Workaround: There is no workaround.

- CSCue92705

  Symptom: The “DHCPD Receive”, “CDP Protocol”, and “Net Background” processes leaks could be seen after disabling **macro auto monitor**.

  Conditions: This symptom is observed in Cisco IOS Release15.0(2)SE1, 2960S, DHCP, CDP traffic, and link flapping.

  Workaround: Configure **no service dhcp** if the switch is not a DHCP server. Configure:

  ```
  device-sensor filter-spec cdp exclude all device-sensor filter-spec dhcp exclude all
  device-sensor filter-spec lldp exclude all
  ```

- CSCuf03690

  Symptom: Onep CDP neighbors are not formed in Cisco IOS Release 15.3(3).

  Conditions: This symptom is observed when onep tries to discover neighbors, it unable to do so since CDP does not give the information correctly.

  Workaround: There is no workaround.

- CSCuf32809

  Symptom: Unconfiguring VLAN causes crash on the Cisco 3900E platform.

  Conditions: Cisco Router 3900E is loaded with Cisco IOS Release 15.3(2.5)T.

  Workaround: Media-mon does not support attaching policy on a L2 interface. When the policy tries to attach on to a L2 interface, a warning is displayed.

- CSCuf77129

  Symptom: Disk errors may be seen on boot up. Files may not be read from the disk leading to the router configuration not being read.

  Conditions: This symptom occurs under random, time-related conditions.

  Workaround: Use the Virtio disk device instead of Integrated Drive Electronics (IDE).

- CSCuf78524

  Symptom: Pings done with size near to the “ppp multilink fragment size” fails when performed from a device connected to the Cisco 2901 router. However, the ping is a success when performed directly from the router.

  Conditions: This symptom is observed when the pings are performed from a device connected to the Cisco 2901 router.

  Workaround: There is no workaround.

- CSCuf93471

  Symptom: After a brief unavailability of LDAP CRL, no new CRL fetches can be performed. The following messages are seen on the interface:

  ```
  Mar 28 08:23:37.988: CRYPTO_PKI: Retrieve CRL using LDAP DIRNAME Mar 28 08:23:37.988:
  CRYPTO_PKI: Failed to send the request. There is another request in progress.
  ```

  Conditions: This symptom was first seen in Cisco IOS Release 15.1(4)M6 and not limited to this release.

  Workaround: Configure the **revocation-check none** command under the affected trustpoint and reload the Cisco router.

- CSCug11921

  Symptom: When VIOS configures **exception flash all flash0:**, VIOS crashes.

  Conditions: Configure **exception flash all flash0:**.

  Workaround: There is no Workaround

- CSCug14423

  Symptom: A packet gets dropped when a spoke-spoke session is triggered in Dynamic Multipoint VPN (DMVPN).

  Conditions: This symptom occurs when a ping is sent using a tunnel interface as the source or the destination.

  Workaround: Send traffic from host-host.

- CSCug17808

  Symptom: Redistributed default route not advertised to EIGRP peer.

  Conditions: This symptom is observed when a Cisco ASR router is rebooted or the route is cleared via the **clear ip route** command, the route disappears form the spokes.

  Workaround: Clearing the EIGRP Neighborship restores the route on the spokes.

- CSCug28860

  Symptom: Missing dial tone when pressing newcall with existing two-way whisper call.

  Conditions: This symptom is observed with whisper intercom only.

  Workaround: There is no workaround, however you can make outgoing call without dial tone.

- CSCug29813

  Symptom: A path confirmation failure occurs for Dual Tone Multifrequency (DTMF) tones.

  Conditions: This symptom occurs in an SIP-SIP call flow in IPv4 and IPv6 scenarios.

  Workaround: There is no workaround.

- CSCug34288

  Symptom: Zero touch upgrade fails.

  Conditions: This symptom is observed when non-VLAN1 scenario with trunk mode configuration and ESM module is connected to another switch.

  Workaround: There is no workaround.

- CSCug43081

  Symptom: If the client and the LDAP server uses NTLMv2 and “ntlm passive” is configured on the ISR, the user authentication fails.

  Conditions: This symptom is observed when the client and the LDAP server uses NTLMv2 and “ntlm passive” is configured on the ISR.

  Workaround: To resolve this issue, configure “ntlm active” on the ISR.

- CSCug45898

  Symptom: A router reload is observed.

  Conditions: The following error message is observed on router reload:

  ```
  489 Bad Event - ‘Malformed/Unsupported Event’ not received
  ```

  Workaround: There is no workaround.

- CSCug58617

  Symptom: Usernames do not show up in CCP Express. Username shows up on a router with default configuration.

  Conditions: The symptom is observed on routers with configurations that break show run | format.

  Workaround: Use default configuration.

- CSCug69107

  Symptom: Crypto session does not come up in EZVPN.

  Conditions: This symptom is observed when a Crypto session is being established.

  Workaround: There is no workaround.

- CSCug72870

  Symptom: HTTP Authproxy Deamon and Malloclite leaks occur.

  Conditions: This symptom occurs when NTLM sessions are authenticated and cleared for more than 10-20 minutes.

  Workaround: There is no workaround.

- CSCug92994

  Symptom: A crash occurs during CDP listener registration for different interfaces.

  Conditions: This symptom is observed when after calling CDP listener API, the router crashes at xos_dm_wait.

  Workaround: Disable CDP listener on management interface and multilink interfaces.

- CSCuh01533

  Symptom: Memory leaks are seen at SADB index list.

  Conditions: This symptom is observed in ISR-G2 and ASR platforms when the configurations are loaded.

Workaround: There is no workaround.

- CSCuh07657

  Symptom: Inter-AS/Aggregate label is not re-originated after the directly connected CE facing interface (in VRF) is shut down.

  Conditions: Inter-AS MPLS VPN set-up with Cisco 7600(PE)Router running on Cisco IOS Release 12.2(33)SRE4.

  Workaround: Downgrade to Cisco IOS Release 12.2(33)SRE3 or earlier.

- CSCuh11115

  Symptom: Not able to session into the Lebowski module from the router.

  Conditions: After the router is booted with default configuration, you will not be able to session into Lebowski Module.

  Workaround: Change the console speed on tty line of the router to 9600 manually.

- CSCuh14012

  Symptom: The crypto session remains UP-ACTIVE after tunnels are brought down administratively.

  Conditions: This symptom occurs in tunnels with the same IPsec profile with a shared keyword.

  Workaround: There is no workaround.

- CSCuh23940

  Symptom: The line status of the 9th port is up/down for HWIC-D-9ESW in the Cisco 3945 Integrated Services Router. The port status displays down/down in Cisco IOS Release 15.3(1)T1 and Cisco IOS Release 15.1(4)M5.

  Conditions: This symptom occurs when the Cisco 3945 Integrated Services Router is used.

  Workaround: There is no workaround.

- CSCuh24040

  Symptom: BGP routes are not marked Stale and considered best routes even though the BGP session with the peer is torn down. A hard or soft reset of the BGP peering session does not help.

  For BFD-related triggering, the following messages are normally produced with the BGP-5-ADJCHANGE message first, and the BGP_SESSION-5-ADJCHANGE message second. Under normal conditions, the two messages will have identical timestamps. When this problem is seen, the order of the messages will be reversed, with the BGP_SESSION-5-ADJCHANGE message appearing first, and with a slightly different timestamp from the BGP-5-ADJCHANGE message. In the problem case, the BGP_SESSION-5-ADJCHANGE message will also include the string “NSF peer closed the session”

  For example when encountering this bug, you would see:

  ```
  May 29 18:16:24.414: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4 Unicast vpn vrf
  VRFNAME topology base removed from session NSF peer closed the session May 29
  18:16:24.526: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD adjacency
  down
  ```

  Instead of:

  ```
  May 29 18:16:24.354: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD
  adjacency down May 29 18:16:24.354: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4
  Unicast vpn vrf VRFNAME topology base removed from session BFD adjacency down
  ```

  Log messages associated for non-BFD triggers are not documented.

Conditions: This symptom is observed when BGP graceful restart is used in conjunction with BFD, but it is possible (but very low probability) for it to happen when BGP graceful restart processing happens when any other type of BGP reset (example: clear command) is in progress.

Affected configurations all include: router bgp ASN ... bgp graceful-restart ...

The trigger is that BGP exceeds its CPU quantum during the processing of a reset, and gives up the CPU, and then BGP Graceful Restart processing runs before BGP can complete its reset processing. This is a very low probability event, and triggering it is going to be highly dependent on the configuration of the router, and on BGP's CPU requirements.

It is not possible to trigger this bug unless BGP graceful-restart is configured.

Workaround: If you are engaged in active monitoring of router logs, and the bug is being triggered by a BFD-induced reset, you can detect this situation by watching for the reversal of log message order described in the Symptom section, and then take manual steps to remedy this problem when it occurs.

On the problematic router, issue the **no neighbor <xxx> activate** command under the proper address-family will clear the stale routes.

The other option is to manually shutdown the outgoing interface which marks the routes as "inaccessible" and hence not been used anymore. This prevents the traffic blackhole but the routes will stay in the BGP table.

More Info: This bug affects all releases where CSCsk79641 or CSCtn58128 is integrated. Releases where neither of those fixes is integrated are not affected.

- CSCuh29095

  Symptom: The cellular interface on IOS gets the same IP address across interface resets but is unable to send data over cellular interface.

  Conditions: This symptom occurs when the modem is subjected to stressful conditions causing SDK timeouts.

  Workaround: Power cycle the modem.

- CSCuh40656

  Symptom: Sessions are stuck in proxy state for more than a day.

  Conditions: This symptom occurs when a stress test is performed.

  Workaround: Use the **clear** command to clear the sessions.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB, although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

  Workaround: Forcibly clear the RIB.

- CSCuh48124

  Symptom: VRF-Aware content scan does not work.

  Conditions: This symptom occurs if ingress or egress is in VRF.

  Workaround: There is no workaround.

- CSCuh51367

  Symptom: An alignment traceback is seen in the L4F code.

Conditions: This symptom occurs when traffic from HTTP/HTTPS goes through Scansafe+l4f.

Workaround: There is no workaround.

- CSCuh56446

  Symptom: START and STOP accounting message for auth-proxy do not carry “Framed-IP-Address”.

  Conditions: This symptom is observed when accounting is enabled for auth-proxy.

  Workaround: There is no workaround.

- CSCuh57618

  Symptom: The gateway sends the following notify message before receiving an unsubscribe request:

  ```
  "Subscription-State Terminated"
  ```

  Conditions: This symptom occurs when the router is loaded with the “c2900-universalk9-mz.SPA.153-2.25.M0.1” image.

  Workaround: There is no workaround.

- CSCuh58624

  Symptom: When invoking a transcoder to convert rtp-nte (RFC2833) DTMF to Inband tones in RTP stream, the outgoing DTMF duration is in the range 25 to 40 ms. This will lead to the digits not being recognised by some IVRs.

  Conditions: This symptom is observed in DSPWare 34.2.7.

  Workaround: There is no workaround.

- CSCuh66763

  Symptom: The following phrases are displayed in English irrespective of locale configured on CME:

  “Next”, “Previous”, “Please modify number”, “Invalid speed dial number”, “Invalid personal speed dial number”, “Invalid blf speed dial number”, “Personal speed dial number can not exceed 32 digits”, “Personal speed dial label can not exceed 30 characters”, “Speed dial number can not exceed 24 digits”, “The record is full”, “Please delete unuse entry”, “Logging Out”, “CME hardware conference”, “CME software conference”, “add party allowed”, “add party not allowed”, “Whisper” “CME group pickup”, “CME pickup”, “Access Mailbox (trnsfVM)”, “Failed to send call to Mobile Phone”, “Live Record is not enable”, “Live Record already in progress”, “Not conference creator”, “Live Record has stopped”, and “Live Record timeout”.

  Conditions: This symptom is observed when you configure a non-English user-locale.

  Workaround: There is no workaround.

- CSCuh68961

  Symptom: In a DO-DO scenario, the CUBE is not able to send re-invite on other leg if the CUBE receives re-invite immediately followed by ACK.

  Conditions: This symptom is observed under the following condition:

  SIP (PSTN) -- CUBE -- SIP -- CUCM -- IP phone transfers to another IP phone Message Sequence in CUBE CUCM --> reINVITE --> CUBE --> reINVITE --> Provider <-- 200OK 200OK <-- ACK --> reINVITE --> --> ACK

  reINVITE from CUCM is not forwarded to the provider

  Workaround: There is no specific workaround. This issue is only seen from the Cisco IOS Release 15.1(4)M and newer.

- CSCuh88777

  Symptom: IPv6 client sending data fails.

  Conditions: This symptom is observed when IPv6 data path fails due to “Failed to obtain acl on MAG”.

  Workaround: There is no workaround.

- CSCuh90005

  Symptom: The following syslog message is seen frequently:

  ```
  CELLWAN-4-SESSION_STATE_MISMATCH_WARN
  ```

  Conditions: This symptom is observed when traffic is sent after the network connection is down. Network connection can go down when the radio signal strength is very poor.

  Workaround: There is no workaround.

  More Info: This issue is only seen with Cisco IOS 153-2.25.M0.6 image

# Caveats for Cisco IOS Release 15.3(2)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.

**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. (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:


- Open Caveats—Cisco IOS Release 15.3(2)T, page 51
- Resolved Caveats—Cisco IOS Release 15.3(2)T, page 77


## Open Caveats—Cisco IOS Release 15.3(2)T

All the caveats listed in this section are open in Cisco IOS Release 15.3(2)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCto08904

  Symptoms: RTP operations fail to run when using multiple operations.

  Conditions: This symptom is observed when more than 16 RTP operations are running. Operations start failing due to scaling issues.


**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Workaround: There is no workaround.

- CSCtr87413

  Symptoms: The static route that is injected by “reverse-route static” in crypto map disappears when the router receives the delete notify from the remote peer. The static route also gets deleted when DPD failure occurs.

  Conditions: This symptom is observed when you configure “reverse-route static” and then receive a delete notify or DPD failure.

  Workaround: Use **clear crypto sa**.

- CSCtr88785

  Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 5.1(4)M1, crashes were experienced in PKI functions.

  Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration.

  Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCts11166

  Symptoms: A router crashes at cce_dp_ipc_save_feature_objects.

  Conditions: This symptom occurs on a Cisco 2951 router running Cisco IOS Release 15.1(2)T1 and Cisco IOS Release 15.1(4)M1.

  Workaround: There is no workaround as the trigger of the issue is unknown.

- CSCtu01606

  Symptoms: HWIC-2SHDSL shows no data when the controller and ATM interface are up on Alcatel and Huawei.

  Conditions: This symptom is observed with HWIC-2SHDSL when the controller and ATM interface are up on Alcatel and Huawei.

  Workaround: Reload the router.

- CSCtx52157

  Symptoms: The SM-ES3G-24-P module installed in a Cisco 3925E chassis shows the status as failed.

  Conditions: This symptom is observed with an SM-ES3G-24-P module installed in a Cisco 3925E chassis.

  Workaround: Reload the SM-ES3G-24-P switch module.

- CSCty09784

  Symptoms: The SS7 link does not come up.

  Conditions: This symptom is observed with the fix of DDTS CSCta18342.

  Workaround: Use the version of IOS that has the issue of “D channel is not recovering after IP flapping IUA”.

- CSCty57970

  Symptoma: A crash occurs when “content-scan out” is unconfigured from the egress interface.

  Conditions: This symptom occurs when “content-scan out” is unconfigured after the router runs continuously for around two days.

  Workaround: There is no known workaround.

- CSCty91566

  Symptoms: A potential memory leak is seen when handling DNS lookup response.

  Conditions: This symptom occurs when handling DNS lookup response.

  Workaround: There is no workaround.

- CSCtz13023

  Symptoms: A SIP gateway may crash with a bus error.

  Conditions: This symptom occurs when the SIP gateway is configured as a SIP registrar. The configurations for this are as follows:

```
voice service voip
  sip
    registrar server
```

  Workaround: There is no workaround available at this time.

- CSCtz54775

  Symptoms: Traffic sourced from a 2901 through a EHWIC-4ESG module resumes forwarding within a maximum of 5 minutes (ARP expiry) instead of 30 seconds (STP convergence time).

  Conditions: This symptom is observed after an STP failover occurs.

  Workaround: Clear the ARP table of the affected interface (after the VLAN is in a forwarding state).

- CSCua05196

  Symptoms: CPU hogs are seen leading to watchdog timeout.

  Conditions: The symptom is observed with a Cisco 2900 router.

  Workaround: Do not enter the **reload** command.

- CSCua26981

  Symptoms: A Cisco ASR router may crash due to a CPU Watchdog upon invocation of “show ip eigrp neighbor detail”.

```
sh ip eigrp nei detail
<snip>
ASR1000-WATCHDOG: Process = Exec
%SCHED-0-WATCHDOG: Scheduler running for a long time, more than the maximum
configured (120) secs.
-Traceback= ...
========= Start of Crashinfo Collection (09:21:44 EST Wed May 9 2012) ==========
```

  Conditions: This symptom occurs when the Cisco ASR router is experiencing rapid changes in EIGRP neighborship, such as during a flap. One way to artificially create this scenario is to mismatch the interface MTU.

  Workaround: There is no workaround.

- CSCua68587

  Symptoms: cvCallVolConnActiveConnection.sip MIB count does not match with what is seen on the CLI.

  Conditions: This symptom is observed with the Cisco ASR 1006 running Cisco IOS XE Release 3.6.0S or Cisco IOS Release 15.2(2)S with the asr1000rp2-adventerprisek9.03.06.00.S.152-2.S image.

  Workaround: There is no workaround.

- 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: This symptom is observed after upgrading to Cisco IOS Release 15.2(3)T.

  Workaround: Connecting via the portal might help.

- CSCub10609

  Symptoms: The offset list does not offset the EIGRP metric properly in EIGRP Classic Mode.

  Conditions: This symptom is observed with Cisco IOS XE Release 3.4S, that is, Cisco IOS Release 15.1(3)S onwards.

  Workaround: In order to get the offset to work correctly, use offsets in multiples of 256.

- CSCub33602

  Symptoms: IGMP query with source IP address 0.0.0.0 triggers a querier election process. As a consequence, the port on which this packet is received is marked as an mrouter port for that VLAN.

  ```
  Router#show ip igmp int vlan 1
  Vlan1 is up, line protocol is up
    Internet address is 1.1.1.1/24
    IGMP querying router is 0.0.0.0 <----

  Router#sh ip igmp snooping mrouter
  vlan            ports
  -----+---------------------------------------
     1  Po1,Po8,Router<-----
  ```

  Conditions: This symptom is observed when IGMP query with source IP address 0.0.0.0 is received.

  Workaround: Configure an ACL to block packets with source IP address 0.0.0.0 and apply it to relevant interfaces.

  ```
  access-list 100 deny   ip host 0.0.0.0 any
      access-list 100 permit ip any any
      int vlan 1
       ip access-group 100 in
  ```

  Further Problem Description: Per RFC 4541, IGMP query with source IP address 0.0.0.0 is used in special cases. When such a query is received by a router, it should not be used in the querier election process.

- CSCub53380

  Symptoms: Legitimate PPP frames are dropped on an async interface, incrementing both “runts” and “unknown protocol drops” in the **show interfaces** command.

  Conditions: This symptom is observed with Cisco ISR G1/G2 platforms running Cisco IOS Release 15.x with the following modules.

  - HWIC-4A/S
  - HWIC-8A/S-232
  - HWIC-8A
  - HWIC-16A

  Workaround: There is no workaround.

- CSCub56842

  Symptoms: The router stops passing IPsec traffic after some time.

  Conditions: This symptom is observed when the **show crypto eli** command output shows that during every IPsec P2 rekey, the active IPsec-Session count increases, which does not correlate to the max IPsec counters displayed in SW.

  Workaround: Reload the router before active sessions reach the max value.

  To verify, do as follows:

```
router#sh cry eli

 CryptoEngine Onboard VPN details: state = Active
 Capability    : IPPCP, DES, 3DES, AES, GCM, GMAC, IPv6, GDOI, FAILCLOSE, HA

 IPSec-Session :  7855 active,  8000 max, 0 failed <<<
```

- CSCub58146

  Symptoms: There is an inconsistency in how NM-16ESW@C2821 handles unregistered multicast groups with IGMP Snooping. It is expected with Cisco IOS is that those groups will be flooded. However, what is observed is that in some VLANs, unregistered groups are flooded and in other VLANs, they are not. Behavior also changes between node reloads and VLAN delete and add (stops flooding). RFC4541 also explicitly requires configuration knob per-interface to enable flooding. On other platforms, this is done by using the **switchport block multicast** command. Cisco C2821 lacks this functionality. An unregistered packet is defined as an IPv4 multicast packet with a destination address that does not match any of the groups announced in earlier IGMP Membership Reports. If a switch receives an unregistered packet, it must forward that packet on all ports to which an IGMP router is attached. A switch may default to forwarding unregistered packets on all ports. Switches that do not forward unregistered packets to all ports must include a configuration option to force the flooding of unregistered packets on specified ports.

  Conditions: This symptom is observed with the following conditions:

  – The L2 access port located at NM-16ESW is receiving IPv4 multicast traffic.

  – Cisco IOS Release 12.4(25a), Cisco IOS Release 15.1(4)M4, and Cisco IOS Release 15.0(1)M8.

  Workaround: There is no workaround.

- CSCub74692

  Symptoms: Path confirmation fails while making H.323 calls in IEC_FORCED_DISENGAGE,IEC_GK_SHUTDOWN and Long call detection scenarios.

  Conditions: This symptom is observed while making H.323 calls in IEC_FORCED_DISENGAGE,IEC_GK_SHUTDOWN and Long call detection scenarios.

  Workaround: Disable CEF using the **no ip cef** command in the GW configuration.

- CSCub83371

  Symptoms: Performance degradation with high CPU is seen on CUBE for SIP-SIP flow-through calls.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T2.13.

  Workaround: There is no workaround.

- CSCub83800

  Symptoms: The Copperopolis Ethernet interface fails to come up with router reload.

Conditions: This symptom occurs when you enable Flow Record with “collect application http host” and Flow Exporter with “source interface xxxx” configurations on the router that has an Ethernet (g.shdsl) interface and reload the router.

Workaround: Apply the configurations again once the router is ready.

- CSCub86574

  Symptoms: The router crashes if PfR and EIGRP are configured on the router.

  Conditions: This symptom is observed with four exit interfaces, that is, two per BR.

  Workaround: There is no workaround.

- CSCub90414

  Symptoms: The device crashes when a block of memory is freed, even though it was not in use.

  Conditions: This symptom occurs when “crypto pki trustpoint” is configured.

  Workaround: Remove the **auto-enroll** command to prevent any other reloads due to this bug. The ultimate resolution is to upgrade Cisco IOS to a release that contains the fix for this bug.

- CSCuc02262

  Symptoms: A crash is seen at tcp_prepare_for_retransmit with the combination of IPv6 and IPv4 traffic.

  Conditions: This symptom is observed in a DMVPN setup with the Cisco 2921 acting as the spoke and the Cisco 3945e as the hub. After passing HTTP traffic using IPv4 as well as IPv6, a crash is seen on the spoke.

  Workaround: There is no workaround.

- CSCuc15092

  Symptoms: When a connection is configured using the **connect** command, the connection goes down after hours of operation. The status of the connection reads “OPER DOWN”.

  Conditions: This symptom occurs when energy-wise is configured on either of the service modules that are inserted in the router.

  Workaround: Reloading the router restores the connection.

- CSCuc18606

  Symptoms: After BGP flap or device reload, the following error is displayed in the log: BGP-3-DELROUTE Unable to remove route for [XYZ] from radix trie

  There is also a reachability issue.

  Conditions: This symptom is observed during BGP flap, router reload, and when changing the NET statement under the ISIS process.

  Workaround: Reconfiguring NET under ISIS or reloading the device may help to resolve the issue.

- CSCuc21859

  Symptoms: Memory leak is seen at ssf_owner_get_feature_sb.

  Conditions: This symptom occurs when the discriminator configuration is with logging, as given in the below examples:

  ```
  logging discriminator <NAME>
  logging host x.x.x.x discriminator DEBUG
  logging discriminator SysLog mnemonics drops NAME
  ```

  Workaround: Remove the discriminator configuration from the logging configuration.

- CSCuc26021

  Symptoms: IKEv2 SAs are not being removed.

  Conditions: This symptom is observed with “no crypto engine” on running traffic or when ISM-VPN crashes and falls back to onboard crypto engine.

  Workaround: Do a “clear cry session” and when SAs are zero, and do a “no crypto engine” for a normal scenario. There is no workaround when ISM-VPN crashes.

- CSCuc60057

  Symptoms: When sending a fax through the Canon machine, through the MGCP BRI, the fax sends three copies instead of one. In the PCM captures taken for the failed fax on the BRI port, an MCF for a EOP is received. However, the machine keeps sending the EOP twice and then disconnects, resulting in the fax being sent thrice.

  Conditions: This symptom is observed only with the Canon l140 machine.

  Workaround: There is no workaround.

  Further Problem Description: Troubleshooting was done as follows:

  1. Changed the DSP firmware by using a different Cisco IOS version. Tried the latest Cisco IOS Release 15.2(2)T.
  2. Tried increasing the signal strength going from the router to the machine by adjusting the gain and attenuation.
  3. Tried reducing the delay between the packets by adjusting the fax play out delay. 4) Stopped any hairpinning by issuing “no local by pass”.

- CSCuc70472

  Symptoms: Compression (V.42bis, V.44) is disabled by “modemcap” for PVDM2-DM. After some time, certain modems start to negotiate V.44/V.42bis and drop those calls before PPP. The number of modems negotiating compression is growing over time, leading to an increase in the drop call rate.

  Conditions: This symptom occurs when the following modemcap is applied:

  ```
  "modemcap entry V32bis_noComp1:MSC=&F0+DCS=0,0;+MS=10,0,4800,14400"
  ```

  or

  ```
  "modemcap entry V32bis_noComp2:MSC=+MS=10,0,4800,14400;%C0"
  ```

  Breakdown:

  ```
  "+DCS=0,0=0,0" - V.44 OFF, V.42bis OFF
    "+MS=10,0,4800,14400" - V.32bis,No V8.bis, min 4800, max 14400
    "%C0" - No compression
  ```

  After reload:

  ```
  Router#sh modem log 0/463 | i compression
   Data compression                69    None
   Data compression                69    None
   Data compression                69    None
   Data compression                69    None  << No compression
  Router#sh modem configuration 0/463 | i S41|S82
      S41 = 137     Compression selection is MNP 5 Retrain and fallback/fall
  forward disabled
      S82 = 128     Break Handling Options/LAPM Break Control = 0x80
      S82 = 21
  ```

  A few hours/days after reload:

```
Router#sh modem log 0/463 | i compression
 Data compression                68    None
 Data compression                68    V44 << Starts to negotiate V.44, even
while disabled by modemcap
 Data compression                68    V44
 Data compression                68    V44
Router#sh modem configuration 0/463 | i S41|S82
    S41 = 139     Compression selection is MNP 5 and V.42 bis
    S82 = 128     Break Handling Options/LAPM Break Control = 0x80
    S82 = 25
```

Workaround: Reload.

- CSCuc73005

  Symptoms: The Cisco IOS firewall stops forwarding RTP packets belonging to an established session after around 30 seconds.

  Conditions: This symptom is observed with a Cisco IOS Zone Based Firewall, with SIP inspection. This issue is seen when RTP traffic is flowing.

  Workaround: There is no workaround.

- CSCuc82169

  Symptoms: The router crashes while configuring “tunnel protection ipsec profile”.

  Conditions: This symptom is observed on the Cisco ASR 1001 when it is configured as a DMVPN Spoke Simulator.

  Workaround: There is no known workaround.

  Further Problem Description: There are more than 900 tunnels created. The router runs out of memory. When the command is entered, the router crashes.

- CSCuc83061

  Symptoms: In an SAF setup with EIGRP, the EIGRP peers are seen flapping continuously when there are mixed TLV version neighbors on a single interface.

  Conditions: This symptom occurs when EIGRP Service-family neighbor-ship flaps are seen at random intervals. There is no definite pattern to these flaps, and they are not restricted to any one peer in the network. This issue is seen when there are two different TLV versions and they are on the same interface, and if service data is greater than 8KB.

  Workaround: There is no workaround. If one of the mixed peers is removed from the interface, the issue will not be seen.

- CSCuc92114

  Symptoms: Logs seen consistently in Cisco 3945 running Cisco IOS Release 15.1(4)M1.

```
Jul 13 10:52:36 MEST: SYS-2-INTSCHED   <
http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi?action=search&counter=0&pa
ging=5&links=reference&index=all&query=SYS-2-INTSCHED>
;  'may_suspend' at level 4  -Process=
"OSPF-100 Hello", ipl= 4, pid= 320
-Traceback= 15CB073z 9081B7z 2851571z 11B7582z 11C275Ez 11C2906z 11C03E3z
1B907B5z 1B9064Cz 1BA5737z 172047Fz 47FFDCz 4D2EEDFz 4D2ED71z 4D2EA2Bz
4D30097z
```

  There is no functional impact.

  Conditions: This symptom occurs when running OSPF over the IPsec tunnel.

  Workaround: There is no workaround.

- CSCud05497

  Symptoms: Rarely, the WCM fails to send the configuration to a WaasExpress device.

  Conditions: This symptom occurs when CM tries to send the configuration to a WaasExpress device. Rarely, the “SSL peer shutdown incorrectly” error is seen, leading to failure to send the configuration.

  Workaround: Go to any WAAS-EXP configuration page and click submit.

- CSCud35669

  Symptoms: IPv6 EIGRP routing updates are not exchanged over the DVTI tunnel with the reventon crypto card active.

  Conditions: This symptom is observed only when reventon is enabled.

  Workaround: Disable reventon and use the on-board crypto engine.

- CSCud51159

  Symptoms: The router becomes inoperable when sending IPv4 multiplex superframes.

  Conditions: This symptom is observed when enabling IP debug commands (**debug ip packet** and **debug ip mux**) and sending ipmux super-frames.

  Workaround: Disable the debug commands by issuing “no debug ip packet” and “no debug ip mux”, whichever is applicable.

- CSCud53041

  Symptoms: CPU degradations are seen for SIP-SIP Flow Through calls in Cisco IOS Release 15.2(2)T2.3.

  Conditions: This symptom is observed between Base Image Cisco IOS Release 15.2(2)T1.14 and Target Image Cisco IOS Release 15.2(2)T2.3, which appears to be due to increased cache miss in the target image. There are no obvious bug fixes committed between Cisco IOS Release 15.2(2)T1.14 and Cisco IOS Release 15.2(2)T2.3, resulting in performance degradation. Investigations are still being done on the degradation seen in Cisco IOS Release 15.2(2)T2.3.

  Workaround: There is no workaround.

- CSCud56450

  Symptoms: PPP drops 20-40 percent of incoming frames.

  Conditions: This symptom is observed when using WIC-1B-S/T-V3 or VWIC2-xMFT-T1/E1 in PPP mode on a Cisco c1900/c2900/c3900/c3900e (or ISR G2) router. Also, the remote device is an NEC router.

  Workaround: Use HWIC-4B-S/T (for BRI) or the VWIC3 card (for T1/E1).

- CSCud61517

  Symptoms: CUBE crashes during a blind-transfer scenario and when “media preference IPv6” is configured.

  Conditions: This symptom occurs only when “media preference IPv6” is configured but is not seen when “media preference IPv4” is configured.

  Workaround: Configure “media preference IPv4”.

- CSCud64082

  Symptoms: Cisco IOS crashes when “show cellular <unit> all” is entered immediately after the CDMA manual activation command without waiting for the activation process to complete.

  Conditions: This symptom occurs only if the following two commands are entered back-to-back:

```
Cellular 0/3/0 cdma activate manual 9111301389 9187111389 122456
show Cellular 0/3/0 all
```

This issue is not seen if the **show** command is entered after the activation process is complete.

Workaround: Wait for manual activation process to complete, that is, the console message indicating activation status is shown on the router console, before issuing any other **show** command.

- CSCud68104

  Symptoms: DTMF Path confirmation fails on SIP gateways for a SIP-SIP call with IPV6 enabled.

  Conditions: This symptom occurs when UUTs are running Cisco IOS Release 15.3(1.7)T.

  Workaround: There is no workaround.

- CSCud68801

  Symptoms: The router is unable to establish a PPP session when using PVDM2-DM over ISDN PRI.

  Conditions: This symptom is triggered by incoming calls from a specific third party device.

  Workaround: Update the firmware to version v3_11 or later.

- CSCud72245

  Symptoms: A traceback is seen, along with a crash when “no crypto ipsec client ezvpn hw-client” is configured.

  Conditions: This symptom occurs when “no crypto ipsec client ezvpn hw-client” is configured.

  Workaround: There is no workaround.

- CSCud73277

  Symptoms: A traceback is seen at rsvp_nat_sb_remove.

  Conditions: This symptom is observed when doing a syn flood attack on a NAT-HA Setup for couple of minutes, and meanwhile doing shut/no shut with an interval of 1 minute on the standby router.

  Workaround: There is no workaround.

- CSCud73571

  Symptoms: After SSO, the router crashes with the memory fragmentation error message.

  Conditions: This symptom occurs after the switchover.

  Workaround: There is no workaround.

- CSCud76796

  Symptoms: A Cisco ISR-G2 router gives tracebacks continuously.

  Conditions: This symptom is observed on a router that has SGT binding and the interface that has SXP configuration flaps, resulting in tracebacks.

  Workaround: There is no workaround.

- CSCud77058

  Symptoms: After some time (a few weeks, months) of proper operation, a Cisco IOS router may start having problems performing CRL check.

  Conditions: This symptom was first observed with Cisco IOS Release 15.x.

  Workaround: Disable CRL checking.

- CSCud78341

  Symptoms: IPv6 NAT cannot allocate a port for IPv4 address and drops v6v4 packets.

Conditions: This symptom occurs when using NAT-PT.

Workaround: There is no workaround.

- CSCud78362

  Symptoms: GW starts to drop calls randomly if you increase simultaneous calls beyond 350.

  Conditions: This symptom occurs if 350 calls are connected on GW, some doing digit collection using Cisco ASR(MRCPv2) and some playing media. Increasing a few more calls triggers the issue of call drops and total calls stay at only 350.

  Workaround: There is no workaround. A patch was provided which fixed the 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.

- CSCud86758

  Symptoms: Router crash is seen.

  Conditions: This symptom occurs when connecting with the IPsec VPN client.

  Workaround: There is no workaround.

- CSCud86856

  Symptoms: The router crashes soon after executing “clear policy-firewall sessions”.

  Conditions: This symptom is observed with ZBF, and only with a large number of sessions.

  Workaround:

  1. Do not use the **clear firewall-policy sessions** command.
  2. Increase the IO memory size using “memory-size iomem 25” (use the right percentage depending on your free processor memory) and reload. However, you may still notice CPUHOGs when executing “clear policy-firewall sessions”.

- CSCud94248

  Symptoms: A Cisco 3945e running Cisco IOS Release 15.1(4) M4 crashes due to a bus error in “show version”.

  Conditions: This symptom is observed with Cisco 3945e running Cisco IOS Release 15.1(4)M4.

  Workaround: There is no workaround.

- CSCue01721

  Symptoms: The ISM-VPN stops with clear session of DMVPN tunnels.

  Conditions: This symptom is observed with site-to-site DMVPN is enabled.

  Workaround: Use the onboard crypto or software crypto engine instead of Reventon.

- CSCue03903

  Symptoms: MGW rejects the call setup(On CRCX) with 402 response.

  ```
  Call Flow OLO -->E1 --> MGW(AS 5400) --> RUDP--> PGW --> MGCP --> MGW (AS
  5400)--> E1 --> OLO
  ```

  This symptom is intermittent in nature. When the issue is active, all the calls through the MGW are rejected with response 402.

Conditions: This symptom is observed with the following conditions:

A sample call failure is given below:

```
Dec 27 10:13:02 172.29.101.20 616169: 607470: Dec 27 10:13:02 CET: MGCP Packet
received from 172.28.100.132:2427--->
Dec 27 10:13:02 172.29.101.20 616170: CRCX 385127563
s5/ds1-1/31@mgwmiit02.noverca.com MGCP 1.0
Dec 27 10:13:02 172.29.101.20 616171: C: 16B9754
Dec 27 10:13:02 172.29.101.20 616172: L: e:off,fxr/fx:t38-loose
Dec 27 10:13:02 172.29.101.20 616173: M: inactive
Dec 27 10:13:02 172.29.101.20 616174: R:
Dec 27 10:13:02 172.29.101.20 616175: S:
Dec 27 10:13:02 172.29.101.20 616176: X: 16F4948A
Dec 27 10:13:02 172.29.101.20 616177: <---
Dec 27 10:13:02 172.29.101.20 616178: 607471: Dec 27 10:13:02 CET: Following
traceback is for INFO ONLY.
Dec 27 10:13:02 172.29.101.20 616179: 607472: Dec 27 10:13:02 CET: -Traceback=
6239B01Cz 62380514z 623782E4z 62370AC4z 6232BD68z 6233141Cz 606DE45Cz 606DE440z
Dec 27 10:13:02 172.29.101.20 616180: 607473: Dec 27 10:13:02 CET: MGCP Packet
sent to 172.28.100.132:2427--->
Dec 27 10:13:02 172.29.101.20 616181: 402 385127563 Call Setup failed
Dec 27 10:13:02 172.29.101.20 616182: <---
Dec 27 10:13:02 172.29.101.20 616183: 607474: Dec 27 10:13:02 CET: MGCP Packet
received from 172.28.100.132:2427--->
Dec 27 10:13:02 172.29.101.20 616184: DLCX 385127567
s7/ds1-4/31@mgwmiit02.noverca.com MGCP 1.0
Dec 27 10:13:02 172.29.101.20 616185: R:
Dec 27 10:13:02 172.29.101.20 616186: S:
Dec 27 10:13:02 172.29.101.20 616187: X: 16F4948E
```

This behavior is suspected to be similar to defect CSCsq35482.

Workaround: MGW reboot will fix the issue, but the issue will recur after a few days.

- CSCue04841

  Symptoms:

  1. The OID SM module reports the “hw-module sm 1 oir-stop” %DXMRVL_FLTMG-7-INTERNAL_ERR error output with a traceback after use.
  2. After reinserting this SM, the related configuration disappears.
  3. When the related configuration is used with “switchport mode trunk”, a crash is seen.

  Conditions: This symptom is observed with the OIRSM module and when doing related configurations.

  Workaround: There is no workaround.

- CSCue17104

  Symptoms: When multipath static routes are added and if they exceed the maximum multipath route limit for the platform, the routes will not be installed in the RIB. Later, when installed routes go unreacheable, the previously uninstalled routes are not added back.

  Conditions: This symptom is observed with multipath static routes. The maximum number of multipath routes for a destination depends on the platform. For instance, it is 8 for Cisco Catalyst 4500 Series.

  Workaround: Issue the following command:

  ```
  clear ip route <route>
  ```

- CSCue20991

  Symptoms:

  1. The “mpls mtu override” option does not work on the Cisco c3900. Packets are dropped with the “%LINK-4-TOOBIG:” error.
  2. The packet size printed in the “%LINK-4-TOOBIG:” error is wrong; it is printing wrong parameter instead of the datagram size.
  3. max_pak_size considered is 1518 even in the case of interface drivers supporting up to 9576.

  Conditions: This symptom is observed with the Cisco c3900 running Cisco IOS Release 15.1(4)M.

  Workaround: Match MPLS MTU exactly with the interface MTU.

- CSCue23898

  Symptoms: A Cisco 2921 router running Cisco IOS Release 15.3(1)T may crash with a bus error.

  Conditions: This symptom occurs while updating the router “Call-manager-fallback” configuration section via Call Manager.

  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.

- CSCue26894

  Symptoms: PfR fails to receive a shutdown notification on the tunnel subinterface.

  Conditions: This symptom has been observed with a Cisco router acting as the PfR Border when a tunnel subinterface is also configured on an PfR external interface.

  Workaround: There is no workaround.

- CSCue28318

  Symptoms: A Cisco router doing authentication proxy may unexpectedly reload when running the **test aaa command** command.

  Conditions: This symptom occurs when the router is using LDAP authentication and has a misconfigured LDAP authentication configuration.

  Workaround: Correct the misconfiguration.

- CSCue28872

  Symptoms: The “C5510-4-NO_RING_DESCRIPTORS No more ring descriptors available on slot X dsp Y.” error is displayed. Intermittently, calls are also disconnected.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T3.

  Workaround: There is no workaround.

- CSCue31051

  Symptoms: The router crashes, indicating memory corruption in chunk memory.

  Conditions: This symptom is observed when CHUNKBADMAGIC may be seen in the crashinfo file or any other chunk memory corruption signature.

  Workaround: There is no workaround.

- CSCue31054

  Symptoms: The NAT device which is in RG-infra HA standby might crash when SIP traffic is passing through the device.

  Conditions: This symptom is observed with the following conditions:

  1. SIP traffic is passing through the NAT device which is in RG-infra active state.
  2. Any trigger for state change from init to standby on the RG-infra peer (other) device causes the crash on the RG-infra active device.

  Workaround: Configure NAT rules in such a way as to stop allowing SIP traffic.

  Further Problem Description: The “no-payload” options or “no ip nat service sip” can be used for achieving the above workaround.

- CSCue32696

  Symptoms: The router crashes, along with the following tracebacks:

```
-Traceback=
      0x6416C9FC[voip_rtcp_server+0x1f4]
      0x63EF3088[r4k_process_dispatch+0x1c]
      0x63EF306C[r4k_process_dispatch+0x0]

-Traceback=
      0x6409DD18[voip_rtcp_multicast_receive_packet+0x50]
      0x6416C9FC[voip_rtcp_server+0x1f4]
      0x63EF3088[r4k_process_dispatch+0x1c]
      0x63EF306C[r4k_process_dispatch+0x0]
```

  From the logs:

```
-Traceback= 6416C9FCz 63EF3088z 63EF306Cz Dec 12 10:40:02.204:
 %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=705D6E80, count=0
-Traceback= 6416C9FCz 63EF3088z 63EF306Cz Dec
12 10:40:02.208: %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=705D604C,
count=0 -Traceback= 6416C9FCz 63EF3088z 63EF306Cz Dec
12 10:40:02.208: %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=6A01CAE8,
count=0 -Traceback= 6416C9FCz 63EF3088z 63EF306Cz
```

  Another thing the user notices prior to a crash is that the device has a very high CPU utilization caused by the RTCP process (up at 99%).

  Conditions: This symptom is observed with the Cisco c3845.

  Workaround: There is no workaround.

- CSCue32707

  Symptoms: “crypto pki export” in PKCS12 format may lead to router crash.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(4)M2.

  Workaround: There is no workaround.

- CSCue32916

  Symptoms: When GETVPN GM is running any Cisco IOS Release 15.x code, registration fails when the crypto map is applied on a GRE tunnel interface which is sourced from a 3G Dialer (Cellular) Interface.

  Conditions: This symptom occurs when the KS is reachable over a GRE tunnel which is sourced from a 3G Dialer interface (Cellular) and the GRE tunnel has the crypto map applied. Crypto map is not applied on any other interface. The crypto local-address has been used as a loopback interface. As per “CSCta50110, GETVPN1.4::GM does not register if crypto map is applied to only tunnel”,

crypto map on tunnel interfaces are supported. The same behavior is not seen when the same tunnel is sourced on an Ethernet or a PPPoE interface. Hence, it is not an issue with the Dialer interface, but with 3G Cellular-based Dialer interfaces. This issue is not seen on any Cisco IOS Release 12.4 codes as well.

Workaround: There is no workaround.

- CSCue38346

  Symptoms: Cisco Unified Border Element running Cisco IOS Release 15.1(4)M1 crashes while handling approximately 300+ SIP calls.

  Conditions: This symptom is observed with Cisco Unified Border Element running Cisco IOS Release 15.1(4)M1.

  Workaround: There is no workaround.

- CSCue40008

  Symptoms: The router crashes when the fair-queue policy is removed from the dialer interface.

  Conditions: This symptom occurs when the fair-queue policy is removed from the dialer interface or a dynamic session.

  Workaround: There is no workaround.

- CSCue40304

  Symptoms: Some senders could not be found in the **show ip rsvp sender vrf ivrf1** command output.

  Conditions: This symptom is observed on configuring senders on spokes.

  Workaround: There is no workaround.

- CSCue41031

  Symptoms: Exta IPsec flow is shown in the “show crypto session” output.

  Conditions: This symptom is observed with the Cisco ASR 1000 RP1 FlexVPN Client.

  Workaround: There is no workaround.

- CSCue41195

  Symptoms: Conf sessions get stuck and dspfarm shut gets stuck at DOWN_PENDING.

```
router#show sccp connections
sess_id    conn_id      stype mode     codec   sport rport ripaddr conn_id_tx

67128607   134235385    conf  inactive UNKNOWN 27720 0     UNKNOWN
67151610   134253266    conf  inactive UNKNOWN 29422 0     UNKNOWN
67151610   134253258    conf  inactive UNKNOWN 31502 0     UNKNOWN


Profile ID = 10, Service = CONFERENCING, Resource ID = 1
Profile Description :
Profile Service Mode : Non Secure
Profile Admin State : DOWN
Profile Operation State : DOWN IN PROGRESS
Application : SCCP   Status : NOT ASSOCIATED
Resource Provider : FLEX_DSPRM   Status : DOWN_PENDING
Number of Resource Configured : 8
Number of Resource Available : 8
Maximum conference participants : 8
Codec Configuration: num_of_codecs:6
Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

```
Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

Conditions: This symptom can be triggered by a CUCM defect CSCtz01408.

Workaround: Reload the router for a temporary workaround.

- CSCue41288

  Symptoms: Some WAAS optimized connections can reach incorrect TCP state and fail removal by keepalive.

  Conditions: This symptom is observed with some WAAS optimized conditions. The trigger for this issue is still being investigated.

  Workaround: Set the affected peers/port to passthrough.

- CSCue42317

  Symptoms: The SIP server options are passed on to the DHCPv6 client even in the case where the DHCPv6 server fails to obtain the prefix information from the Radius server.

  Conditions: This symptom is observed when the DHCPv6 Server fails to obtain the prefix from the Radius Server. That is, when NOPREFIX_AVAIL is received by the Server from the Radius Server.

  Workaround: There is no workaround.

- CSCue43297

  Symptoms: Outpulse Transfer TBCT is broken.

  Conditions: This symptom occurs when a call comes from the E1 line to the Ingress gateway, where survivability is configured. This issue is seen when TBCT is configured, and the outpulse of digits is not happening from the Gateway.

  Workaround: There is no workaround.

- CSCue43655

  Symptoms: Random DSP crash occurs where a T.38 call is switched to FAX when FAX is not configured.

  Conditions: This symptom occurs when a T.38 call is switched to FAX when FAX is not configured.

  Workaround: There is no workaround.

- CSCue46377

  Symptoms: A crash occurs after entering “sh ccm-manager music-on-hold”.

  Conditions: This symptom occurs after entering “sh ccm-manager music-on-hold”.

  Workaround: There is no workaround.

- CSCue48254

  Symptoms: After an upgrade from Cisco IOS Release 15.0M to Cisco IOS Release 15.2M, the CPU usage with the same traffic load is increased.

  Conditions: This symptom is observed with the Cisco ISR-G2 platform.

  Workaround: There is no workaround.

- CSCue48385

  Symptoms: The router has an unexpected reload at the CCSIP_SPI_CONTROL process.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(26)T6.

  Workaround: There is no workaround.

- CSCue48419

  Symptoms: The Cisco AS5350 stops processing calls on PRI with a signaling backhaul from PGW. In the packet trace, there is no q931message from PGW. Further analysis shows that as5350 sends a q_hold (0x5)message in BSM, causing peer (PGW) to stop sending signaling traffic. However, there is no BSM_resume message or BSM_reset sent after it. Hence, PGW is stuck in this condition. There was earlier defect for CSCts75818 with similar symptoms in U-state.

  Conditions: This symptom is observed due to some RUDP timing issues that cause BSM session switchover.

  Workaround: Reload the Cisco AS5350 (but only when CU notices the outage). Also, shutting both Ethernet interfaces may help, but this workaround has not been tested.

- CSCue49424

  Symptoms: The device crashes repeatedly on bootup.

  Conditions: This symptom occurs due to a Kron job that runs on bootup. The Kron job invokes a chat-script that unlocks a cellular card.

  Workaround: Use EEM instead of Kron.

- CSCue50205

  Symptoms: The Masterkey to encrypt preshared keys goes missing unexpectedly.

  Conditions: This symptom is observed with the Masterkey.

  Workaround: There is no workaround.

- CSCue52864

  Symptoms: When the Output Service policy is applied to the serial links of the HWIC-xCE1T1-PRI card, the serial links bounce.

  Conditions: This symptom is observed with the following conditions:

  1. When more than two channel groups are applied to the same controller port.
  2. When the serial links are congested.
  3. When the Output Service policy is applied to more than two serial links of the same controller port.

  Workaround: Do not apply the Output Service policy.

- CSCue52994

  Symptoms: Ping fails with bidirectional data traffic between pagents.

  Conditions: This symptom is observed with a Cisco IOS Release 15.2(4)M2.8 image.

  Workaround: There is no workaround.

- CSCue53677

  Symptoms: A call fails as the expected number of RTP connections are not found in the gateway due to the failure of media negotiation for an incoming PRACK.

  Conditions: This symptom occurs when the router is loaded with c2951-universalk9-mz.SPA.153-1.17.T0.1.

  Workaround: There is no workaround.

- CSCue53686

  Symptoms: The ISM Encryption module consumes fragmented packets that need further fragmentation prior to encryption when using a crypto map.

Conditions: This symptom is observed with a LAN-to-LAN crypto map-based IPsec tunnel. A large IP fragment traverses the IPsec tunnel, but it needs to be fragmented prior to encryption.

Workaround: Disable the ISM module and use the onboard crypto engine.

- CSCue54104

  Symptoms: A crash is seen intermittently.

  Conditions: This symptom occurs after 60+ PRI calls take place. The exact conditions are still being investigated.

  Workaround: There is no known workaround. Downgrade to Cisco IOS Release 15.1(4)M3 or earlier releases.

- CSCue56272

  Symptoms: The Cisco ISR crashes due to watchdog timeout after SYS-3-CPUHOG errors with a traceback.

  Conditions: This symptom is observed with voice traffic through the router.

  Workaround: There is no workaround.

- CSCue59775

  Symptoms: The device crashes.

  Conditions: This symptom is observed when the service-policy is removed.

  Workaround: There is no workaround.

- CSCue59834

  Symptoms: A Cisco 3925 (ISR-G2) configured for crypto tunnels using the onboard VPN module may crash.

  Conditions: This symptom is observed when in the crashinfo file/console logs, there may be messages pointing to “reventon”, which is the firmware that operates this onboard module. This may be seen, along with badshare messages.

  ```
  000259: *Jan 21 09:08:34.966:  [reventon_rx_ib_no_decrypt_common]:
  tx_ctx->flags: 0x0
  000260: *Jan 21 09:08:34.966: %SYS-2-BADSHARE: Bad refcount in retparticle,
  ptr=3C6010D3, count=0
  ```

  Workaround: The workaround is not yet known but possibly disabling this card may be advisable. If this is the only VPN module installed and this card is disabled, CPU usage will increase and possibly to very high levels.

- CSCue62292

  Symptoms: The router crashes with an Address error with the following messages before the crash:

  ```
  Di0 DDR: dialer shutdown complete
  %DIALER-6-BIND: Interface Vi3 bound to profile Di0
  %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
  %LINK-3-UPDOWN: Interface Virtual-Access3, changed state to up
  %DIALER-6-UNBIND: Interface Vi3 unbound from profile Di0

  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x22473FA0
  ```

  Conditions: This symptom is observed when a Dialer interface is unbound.

  Workaround: There is no workaround.

- CSCue63763

  Symptoms: A blind transfer scenario over T1 PRI fails.

Conditions: This symptom is observed from Cisco IOS Release 15.3(1.11)T.

Workaround: There is no workaround.

- CSCue63811

  Symptoms: Memory leaks are seen while testing Call Transfer for a video call.

  Conditions: This symptom occurs when VCC is enabled.

  Workaround: There is no workaround.

- CSCue65130

  Symptoms: 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.

- CSCue65498

  Symptoms: Wrong CIR is getting cloned to the VA interface.

```
Dialer1
   Service-policy output: OPT3-DIALER-4b-TR25
     Class-map: CRI-OUT (match-any)
       police:
           cir 8 %
           cir 819000 bps, bc 25593 bytes          <<<<<

  Virtual-Access3
   Service-policy output: OPT3-DIALER-4b-TR25
     Class-map: CRI-OUT (match-any)
       police:
           cir 8 %
           cir 8000000 bps, bc 250000 bytes        <<<<<
```

  Conditions: This symptom is observed with the PPPoE dialer/client configuration.

  Workaround: Remove and reapply the service-policy under the Dialer interface.

- CSCue65931

  Symptoms: NTLM sessions do not scale under stress (for example, Curl loader).

  Conditions: This symptom occurs when a large number of sessions (>500) are being authenticated at the same time. Connection IDs get exhausted, leading to tracebacks.

  Workaround: There is no workaround.

- CSCue65965

  Symptoms: Device crash is seen with the DSP module.

  Conditions: This symptom is observed with the DSP module with the Cisco c2821

  Workaround: There is no workaround.

- CSCue66002

  Symptoms: The router crashes due to a SIP timer expiry

  Conditions: This symptom is triggered by a SIP generic timer expiry.

  Workaround: There is no known workaround.

- CSCue67372

  Symptoms: GM ignores the negotiation packet which makes negotiation fail.

  Conditions: This symptom is observed with the Cisco 7206VXR running Cisco IOS Release 12.4(24)T7 with VAM2+.

  Workaround: There is no workaround.

- CSCue68127

  Symptoms: A Cisco 3845 router will crash due to IO memory corruption.

  Conditions: This symptom occurs when WebVPN is enabled and the router receives a TLS hello packet from the server.

  Workaround: There is no workaround.

- CSCue68318

  Symptoms: The ATM interface and subinterface are up/up but are unable to access the Internet.

  Conditions: This symptom occurs only when the IP address of that ATM interface is configured under the EIGRP process.

  Workaround: Downgrade to Cisco IOS Release 15.0(1)M8.

- CSCue68499

  Symptoms: A crash is observed with a H323-H320 video call.

  Conditions: This symptom is observed with the latest image with a H323-H320 video call.

  The topology is as follows:

  ```
  99xx Phone ---> CUCM --- H323 --- OGW --- H320 --- TGW ---> H323 ---> CUCM2
  --->99xx
  ```

  There is already one SR with H320 video call, that is, SR-623302329.

  Crash observed image: c2800nm-ipvoice_ivs-mz.153-1.T.InternalUseOnly

  There is already one SR with H320 video call, that is, SR-623302329. The crash is not observed with c2800nm-ipvoice-mz.151-4.M5.

  Crash observed image: c2800nm-ipvoice_ivs-mz.153-1.T.InternalUseOnly

  The crash decode is as follows:

  ```
  0x40070A00:abort(0x400709f8)+0x8
  0x4006F8BC:crashdump(0x4006f7bc)+0x100
  0x43FF5AF0:validblock(0x43ff54bc)+0x634
  0x43FDB408:__free(0x43fdb230)+0x1d8
  0x442935C4:voip_rtcp_remove_ccb(0x442932a8)+0x31c
  0x44294EBC:voip_rtcp_send_destroy(0x44294a30)+0x48c
  0x419555A4:h323_destroy_rtp_stream(0x419553e8)+0x1bc
  0x419C8A70:cch323_free_add_olc(0x419c89ac)+0xc4
  0x41969844:cch323_call_generic_cleanup(0x41968d1c)+0xb28
  0x41997664:handle_release_event(0x41997508)+0x15c
  0x4198CA04:run_h225_sm(0x4198c6f0)+0x314
  0x419F81AC:cch323_iev_queue_service(0x419f803c)+0x170
  0x419762E4:cch323_process_external_event(0x419753d8)+0xf0c
  0x4194950C:cch323_ct_main(0x419491ac)+0x360
  0x43FC9458:r4k_process_dispatch(0x43fc943c)+0x1c
  0x43FC943C:r4k_process_dispatch(0x43fc943c)+0x0
  ```

  Workaround: There is no workaround.

- CSCue68761

  Symptoms: A leak in small buffer is seen at ip_mforward in Cisco IOS Release 15.1(4)M3.

  Device: Cisco 2911

  Cisco IOS: c2900-universalk9-mz .SPA.151-4.M3.bin

  Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3.

```
------------------ show buffers ------------------


Buffer elements:
     156 in free list (500 max allowed)
     11839912 hits, 0 misses, 617 created

Public buffer pools:
Small buffers, 104 bytes (total 45187, permanent 50, peak 45187 @ 10:04:00):
     0 in free list (20 min, 150 max allowed)
     7968057 hits, 202704 misses, 2128 trims, 47265 created
     71869 failures (680277 no memory)

------------------ show buffers usage ------------------


Statistics for the Small pool
Input IDB    :        Mu1 count:    45180
Caller pc    : 0x22CF95C4 count:    45180
Resource User:   IP Input count:    45180
Caller pc    : 0x22381654 count:        2
Resource User:       Init count:        2
Output IDB   :        Mu1 count:        4
Caller pc    : 0x2380114C count:        4
Resource User: PIM regist count:        4
Number of Buffers used by packets generated by system: 45187
Number of Buffers used by incoming packets:

++++++++++++++++++++++++++++small buffer
packet++++++++++++++++++++++++++++++++

<snip>

Buffer information for Small buffer at 0x2A815220
  data_area 0xD9DEB04, refcount 1, next 0x0, flags 0x2080
  linktype 7 (IP), enctype 16 (PPP), encsize 2, rxtype 1
  if_input 0x30F21520 (Multilink1), if_output 0x0 (None)
  inputtime 00:02:46.212 (elapsed 05:55:11.464)
  outputtime 00:01:22.632 (elapsed 05:56:35.044), oqnumber 65535
  datagramstart 0xD9DEB56, datagramsize 38, maximum size 260
  mac_start 0xD9DEB56, addr_start 0x0, info_start 0xD9DEB58
  network_start 0xD9DEB58, transport_start 0xD9DEB6C, caller_pc 0x22CF0044

  source: 10.131.124.33, destination: 224.0.1.40, id: 0x55F0, ttl: 11,
  TOS: 192 prot: 17, source port 496, destination port 496

0D9DEB56:                   002145C0 002455F0          .!E@.$Up
0D9DEB5E: 00000B11 F14C0A83 7C21E000 012801F0  ....qL..|!`..(.p
0D9DEB6E: 01F00010  82211200  00000000 000000    .p...!.........
```

  Workaround: There is no known workaround. Reboot frees up memory.

- CSCue69527

  Symptoms: More than 95 SCCP controlled FXS ports cannot be configured on the Cisco VG350.

The debug output for “debug ccm-manager config-download errors” is as follows:

```
cmapp_sccp_gw_start_element_handler: warning - max number of interfaces reached.
```

Conditions: This symptom occurs when configuring more than 95 SCCP FXS ports on the Cisco VG350 using CUCM.

Workaround: There is no workaround.

- CSCue69535

  Symptoms: The Dynamic Performance Monitor fails to report the metrics.

  Conditions: This symptom is observed after recreating the interface.

  Workaround: There is no workaround.

- CSCue70449

  Symptoms: Ping fails for the second peer from the cme1 router.

  Conditions: This symptom occurs when applying crypto map voice to the interfaces.

  Workaround: There is no workaround.

- CSCue70469

  Symptom: During voice to fax switchover, if the SDP contains the first m-line as audio, and the second as fax, the call goes through fine. If the first m-line is fax and the second one is audio, CUBE sends malformed SDP to CUCM, resulting in call failure.

  Conditions: This symptom occurs during voice to fax switchover, if SDP contains two m-lines, CUBE rejects the call with 488. This behavior has been changed in Cisco IOS Release 15.3(2)T. In the new behavior, during voice to fax switchover, if the SDP contains the first m-line as audio, and the second as fax, the call goes through fine. If the first m-line is fax and the second one is audio, CUBE sends malformed SDP to CUCM, resulting in call failure.

  Workaround: Always send first the m-line as audio and the second m-line as fax.

  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:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCue70922

  Symptoms: A Cisco 3900e series router may experience a nested crash with ISDN.

  ```
  Unexpected exception to CPU: vector D, PC = 0x7B29FD
    Nested write_crashinfo call (2 times)

    No warm reboot Storage
    *** System received a Bus Error exception ***
    signal= 0xa, code= 0xd, context= 0x9cc1740
    PC = 0x2456e1, Vector = 0xd, SP = 0x63692ec
  ```

  Conditions: This symptom is observed with a Cisco 3900e series router.

  Workaround: Disable the PRI or disable any ISDN debugs (undebug all).

- CSCue74346

  Symptoms: Path confirmation failure is seen with mid-call signaling block enabled.

Conditions: This symptom is observed from Cisco IOS Release 15.3(1.11)T. This issue is seen only for IPv6 cases.

Workaround: There is no workaround.

- CSCue75018

  Symptoms: Through SNMP, traps are not getting configured.

  Conditions: This symptom occurs on setting up an SNMP session with the information provided by the mpls-driver input file.

  Workaround: There is no workaround.

- CSCue75022

  Symptoms: IPsec SAs are not getting deleted even after removing the ACL.

  Conditions: This symptom is observed with IPSec SAs.

  Workaround: There is no workaround.

- CSCue75404

  Symptoms: Files beyond a certain size with certain websites such as yahoo.com cannot be attached.

  Conditions: This symptom is observed with files beyond a certain size.

  Workaround: There is no workaround.

- CSCue75557

  Symptoms: Ping failure is seen between the ISDN BRI interfaces OPF UUT and peer.

  Conditions: This symptom occurs on loading the Cisco IOS Release 15.3(1)T0.1 image.

  Workaround: There is no workaround.

- CSCue75860

  Symptoms: C3900-SPE250/K9 gets reloads when changing the trunk to access mode.

  Conditions: This symptom is observed with the Cisco IOS Release 153.(1.15)T image.

  Workaround: There is no workaround.

- CSCue76102

  Symptoms: Redistributed internal IPv6 routes from v6 IGP into BGP are not learned by the BGP neighboring routers.

  Conditions: This symptom occurs because of a software issue, due to which the internal IPv6 redistributed routes from IGPs into BGP are not advertised correctly to the neighboring routers, resulting in the neighbors dropping these IPv6 BGP updates in inbound update processing. The result is that the peering routers do not have any such IPv6 routes in BGP tables from their neighbors.

  Workaround: There is no workaround.

- CSCue77444

  Symptoms: Memory leak is caused by the “IP Input” process.

  Conditions: This symptom occurs when enabling X25 routing on a router and initiating TCPConnect IP SLA probe on the router’s IP and port 1998.

  Workaround: Change the port to one other than 1998.

- CSCue79042

  Symptoms: Unexpected reload occurs on the Cisco 3900e.

```
Unexpected exception to CPU: vector D, PC = 0x4BF1884
```

Conditions: This symptom is observed with the Cisco 3935 running Cisco IOS Release 15.2(4)M1.

Workaround: There is no workaround.

- CSCue79402

  Symptoms: The router fails to save the last **clock set ...** command even after applied **clock update-calendar** command.

  Conditions: This symptom occurs when you powercycle the router.

  Workaround: Re-enter **clock set ...** and **clock update-calendar** commands, after the router is rebooted.

- CSCue80178

  Symptoms: The EZVPN client does not get associated and no SAs are found.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(1)T0.1 image.

  Workaround: There is no workaround.

- CSCue80261

  Symptoms: The recv error count is not correct in “show crypto ipsec sa ident”.

  Conditions: This symptom occurs after configuring crypto map.

  Workaround: There is no workaround.

- CSCue80270

  Symptoms: Tracebacks are seen for CME supplementary service scenarios.

  Conditions: This symptom occurs while doing media path confirmation. Only tracebacks are seen and the functionality is not impacted with this traceback.

  Workaround: There is no workaround.

- CSCue80662

  Symptoms: EZVPN(hw-client): IPSec connection is terminated with PFS on the client.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(1)T0.1 image on the router.

  Workaround: Remove the PFS.

- CSCue80878

  Symptoms: The router fails to switch to “routing-context vrf <name>” even when all the VRF-related configurations are present.

  Conditions: This symptom is observed when a VRF is configured and used in EIGRP. This condition has been verified with “show eigrp address-family ipv4 vrf <name> topology” as well.

  Workaround: There is no workaround.

- CSCue81874

  Symptoms: There is a counter issue in “show interface summary” with VWIC2-2MFT-T1/E1. The user has a lab with the below topology :

```
2901 ---------Multilink with 2 T1's (VWIC2-2MFT-T1/E1)-----------------2901
  |
                  |
  |
                  |
  |-----------------------Voice call Generator---------------------------------|
```

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

2901-----------------Multilink with 2 T1's (HWIC-2T)-------------------2901
  |
                |
  |
                |
  |------------------------Voice call Generator-------------------------------|
```

1. With VWIC2-2MFT-T1/E1, the output of “show interface summary” and “show interface” shows asymmetric counters (Bits/Sec and Packets/sec) in both input and output directions on both Gigabit and Multilink interfaces.
2. With HWIC-2T, the output of “show interface summary” and “show interface” shows symmetric counters (Bits/Sec and Packets/sec) in both input and output directions on both Gigabit and Multilink interfaces.
3. There was an earlier bug CSCtz48125 for the counter issue, but according to the customer, the issue was not fixed.
4. For Cisco IOS Tested Cisco IOS Release 15.1(4)M5 and Cisco IOS Release 15.1(3)T, different counters with different Cisco IOS versions are seen, but the number of voice calls are the same.

Conditions: This symptom is only observed with RTP traffic and is not seen with nonvoice/data traffic .

Workaround: There is no workaround.

- CSCue83631

  Symptoms: The Gateway fails to send 400 Invalid CSeq Number for SUBSCRIBE.

  Conditions: This symptom occurs when UUTs are loaded with c2900-universalk9-mz.SSA.153-2.3.T.

  Workaround: There is no workaround.

- CSCue83683

  Symptoms: The Agent Greeting is not played out.

  Conditions: This symptom is observed with the Agent Greeting Call Flow using CVP.

  Workaround: There is no workaround with this build.

- CSCue87185

  Symptoms: The DF flag message is not received with “crypto ipsec df-bit copy”.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(2.3)T image.

  Workaround: There is no workaround.

- CSCue87244

  Symptoms: DNS SRV does not receive the expected output.

  Conditions: This symptom is observed when UUTs are loaded with c2900-universalk9-mz.SSA.153-2.3.T.

  Workaround: There is no known workaround.

- CSCue87690

  Symptoms: After seeing repeated CPUHOG errors, the router crashes due to a watchdog timeout at “AFW_application_process”.

  Conditions: This symptom occurs when voice traffic is flowing through the router.

Workaround: There is no workaround.

- CSCue88359

  Symptoms: The join-group message is not forwarded when the IGMP snooping feature is on. This issue is not seen when IGMP snooping is disabled.

  Conditions: This symptom occurs when IGMP Snooping is enabled.

  Workaround: There is no workaround.

- CSCue88659

  Symptoms: When installing a new signature file, a router reports traceback of Cisco IOS-IPS.

  Conditions: This symptom occurs when installing a new signature file.

  Workaround: There is no workaround.

- CSCue89019

  Symptoms: Datapath is broken since the traffic exit via a wrong VRF.

  Conditions: This symptom is observed with the following conditions:

  - VRF-aware IPsec.
  - ISM module enabled.

  Workaround: Disable ISM and use the onboard crypto engine instead.

- CSCue89459

  Symptoms: Path confirmation fails for EO-EO and DO-DO escalation.

  Conditions: This symptom is observed with EO-EO and DO-DO cases.

  Workaround: There is no workaround.

- CSCue89532

  Symptoms: Tracebacks are seen after modem call.

  Conditions: This symptom occurs after modem call with STCAPP services enabled.

  Workaround: There is no workaround.

- CSCue89674

  Symptoms: Expected debugs are not seen in 183, 180, and OK.

  Conditions: This symptom occurs when the router is loaded with c2900-universalk9-mz.SSA.153-2.3.T.

  Workaround: There is no workaround.

- CSCue89779

  Symptoms: A FlexVPN spoke configured with an inside and/or a front-door VRF may have problems with spoke-to-spoke tunnels. During tunnel negotiation, two Virtual-access interfaces are created (while only one is needed); the one in excess may fail to cleanup correctly. As a result, the routes created by the NHRP process may lead to loss of traffic, or traffic may continue to flow through the Hub.

  Conditions: This symptom is observed when the VRF is used as IVRF or FVRF for the affected FlexVPN.

  Workaround: There is no workaround.

- CSCue89803

  Symptoms: The Cisco ISR G2 with reventon does not report IPv6 TBAR errors. This issue can be detected several ways:

  – GM error recovery is not triggered.
  – “show crypto gdoi gm replay” does not show TBAR errors.
  – “show log” does not show IPv6 TBAR errors.

  Conditions: This symptom is observed when two or more GMs are out of sync (TBAR counters are out of sync) and sending IPv6 traffic with reventon enabled.

  Workaround: Disable reventon and use the onboard crypto engine or software crypto engine.

- CSCue89814

  Symptoms: GM error recovery does not get triggered when GM is receiving invalid SPI packets. The GM log does not show any invalid SPI packet syslog messages.

  Conditions: This symptom occurs when GM receives GETVPN IPv6 packets with an invalid SPI.

  Workaround: Disable reventon and use the onboard crypto engine or software crypto engine.

- CSCue90832

  Symptoms: CUBE sends an invalid error response when the dial peer is busied out.

  Conditions: This symptom is observed from Cisco IOS Release 15.3(2.2)T.

  Workaround: There is no workaround.

- CSCue91313

  Symptoms: GETVPN VRF-aware GM crashes.

  Conditions: This symptom occurs after reregistration of 44 IPv4 GDOI groups is completed.

  Workaround: There is no workaround.

- CSCue91847

  Symptoms: The cbarge functionality does not work as expected.

  Conditions: This symptom is observed from Cisco IOS Release 15.3(2.2)T.

  Workaround: There is no workaround.

# Resolved Caveats—Cisco IOS Release 15.3(2)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.3(2)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCso88138

  Symptoms: The RSVP interface stays down after configuring IP on the dot1q subinterface.

  Conditions: This symptom is observed with the RSVP interface timing.

  Workaround: Shut/no shut the interface.

- CSCta80024

  Symptoms: The router crashes while using the **string repeat** command with the biggest number in the TCL shell.

Conditions: This symptom occurs when the **string repeat** command is used with the biggest number. This issue also depends on the string being used. For example, the below commands in the TCL shell will lead to crashing of the router.

```
proc demo foo "set bar [string repeat {$foo} 255]" demo [string repeat a 16843010];
concat
```

Workaround: There is no workaround.

- CSCtf50867

  Symptoms: The router reloads at iprouting_is_hdvrf_idb.

  Conditions: This symptom is observed when configuring “pri-group nfas_d” with Cisco IOS Release 15.1(01.05)T.

  Workaround: There is no workaround.

- CSCtg22670

  Symptoms: Cisco 2900/3900 routers do not detect spurious memory accesses.

  Conditions: This symptom occurs when a bug is present that causes a read from the lowest 16 KB of memory.

  Workaround: There is no workaround.

- CSCtg82170

  Symptoms: The IP SLA destination IP/port configuration changes over a random period of time. This issue is hard to reproduce but has been reported after upgrading to Cisco IOS Release 15.1(1).

  So far, it only seems to have affected the destination IP and port. The destination IP may be changed to an existing destination IP that has already been used by another probe. The destination port is sometimes changed to 1967, which is reserved for IP SLA control packets. Other random destination ports have also been observed to replace the configured port for some of the IP SLA probes. Each time when the change happens, many of the IP SLA probes will stop running.

  Conditions: This symptom is observed in Cisco IOS Release 15.1(1)XB and Cisco IOS Release 15.1(1)T. Other Cisco IOS versions may also be affected.

  Workaround: A possible workaround is to downgrade to any Cisco IOS versions older than Cisco IOS Release 15.1.x.

- CSCtk00181

  Symptoms: Password aging with crypto configuration fails.

  Conditions: This 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.

- CSCtn16281

  Symptoms: Mesh AP crashes on BVI restart by DHCP.

  ```
  *Feb  9 04:00:45.911: %MESH-6-ADJ_VIDB_LINK: Mesh neighbor 0021.1bc0.XXXX VIDB
  Virtual-Dot11Radio2 dot1x control
  *Feb  9 04:01:03.199: %DHCP-5-RESTART: Interface BVI1 is being restarted by DHCP

  *Feb  9 04:01:06.023: %MESH-6-CAPWAP_RESTART: Mesh Capwap re-started

  === Start of Crashinfo Collection (04:01:06 UTC Wed Feb 9 2011) ===
  ```

  Conditions: This symptom is a corner case and is a low probability crash.

Workaround: There is no workaround. AP will reload and rejoin the controller.

- CSCtq23960

  Symptoms: A Cisco ISRG2 3900 series platform using PPC architecture crashes and generates empty crashinfo files:

```
show flash: all

-#- --length-- -----date/time------ path
<<snip>>
2            0 Mar 13 2011 09:40:36 crashinfo_<date>
3            0 Mar 13 2011 12:35:56 crashinfo_<date>
4            0 Mar 17 2011 16:14:04 crashinfo_<date>
5            0 Mar 21 2011 05:50:58 crashinfo_<date>
```

  Conditions: This symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

  Workaround: There is no workaround.

- CSCtq41512

  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to Multi-frame established.

  Conditions: This symptom occurs 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.

- CSCtr47084

  Symptoms: Changing a zone from the multilink interface and replacing the entire configuration by doing a **config replace flash:***config-file-name* crashes the router.

  Conditions: This symptom is observed when traffic is running.

  Workaround: There is no workaround.

- CSCts01653

  Symptoms: Spurious memory access is seen on the video monitoring router.

  Conditions: This symptom occurs after recreating the interface.

  Workaround: There is no workaround.

- CSCts47776

  Symptoms: The router crashes due to Mediatrace performance monitor debug.

  Conditions: This symptom is observed with the debug performance monitor database.

  Workaround: There is no workaround.

- CSCts60458

  Symptoms: There is a memory leak in PfR MIB.

  Conditions: This symptom occurs when the PfR is configured.

  Workaround: There is no workaround.

- CSCts75737

  Symptoms: Tracebacks are seen at swidb_if_index_link_identity on the standby RP.

  Conditions: This symptom is observed when unconfiguring and reconfiguring “ipv4 proxy-etr” under the router LISP.

Workaround: There is no workaround.

- CSCts89761

  Symptoms:

  1. Inline service policy configuration: Unable to configure monitor parameters once the flow monitor is specified. See the following example:

```
Router(config)#interface GigabitEthernet0/2/1
Router(config-if)#service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)#match access-group 110
Router(config-if-spolicy-inline)#flow monitor FM_DEF_TCP <--- After this
point,
all configs will print out an error message
Router(config-if-spolicy-inline)#monitor parameters <----- Not accepted
Router(config-spolicy-inline-mparam)#interval duration 10 <-------- Not
accepted
Router(config-spolicy-inline-mparam)#history 5 <------------ Not accepted
```

  2. Noninline service policy: Unable to change monitor parameters once the flow monitor is bound to a policy-map and attached to an interface. See the following example:

     If an attempt is made to change monitor parameters of an already attached policy as below, it will be rejected.

```
UUT_451(config)#policy-map type performance-monitor VM_POLICY
UUT_451(config-pmap)#class VM_CLASS
UUT_451(config-pmap-c)#flow monitor VM_MONITOR
UUT_451(config-pmap-c)#monitor parameters
UUT_451(config-pmap-c-mparam)#history 6 <----------- Error message will show
up
if previous history value is different
UUT_451(config-pmap-c-mparam)#interval duration 7 <----- Error message will
show up if previous interval duration is different
UUT_451(config-pmap-c-mparam)#react 102 mrv <-------- Error message will show
up if this react was not configured before or if the subsequent command
changes
the threshold value of the already-configured react.
```

  Conditions:

  1. This symptom is seen when configuring an inline service policy for the performance monitor on the Cisco ASR platform.
  2. This symptom is seen when modifying monitor parameters of a noninline service policy for the performance monitor on a Cisco ASR platform.

  Workaround:

  1. To configure the inline service policy, always specify all monitor parameters first and put the **flow monitor** *monitor name* command as the last command in the configuration.
  2. To change the monitor parameters, remove the service-policy by using the **no service-policy** command, make your changes, and then reattach the service-policy.

  The above configuration restrictions do not apply if the enclosing policy-map is not attached to any interface. Also, the changes do not apply if you specify an “empty” flow monitor, for example, a flow monitor without an enclosing valid flow record.

- CSCtt15963

  Symptoms:

  1. Inline service policy Configuration: Unable to configure monitor parameters once the flow monitor is specified. See the following example:

```
Router(config)#interface GigabitEthernet0/2/1
Router(config-if)#service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)#match access-group 110
Router(config-if-spolicy-inline)#flow monitor FM_DEF_TCP <--- After this
point,
all configs will print out an error message
Router(config-if-spolicy-inline)#monitor parameters <----- Not accepted
Router(config-spolicy-inline-mparam)#interval duration 10 <-------- Not
accepted
Router(config-spolicy-inline-mparam)#history 5 <------------ Not accepted
```

2. Noninline service policy: Unable to change monitor parameters once the flow monitor is bound to a policy-map and attached to an interface. See the following example:

   If an attempt is made to change monitor parameters of an already attached policy as below, it will be rejected.

```
UUT_451(config)#policy-map type performance-monitor VM_POLICY
UUT_451(config-pmap)#class VM_CLASS
UUT_451(config-pmap-c)#flow monitor VM_MONITOR
UUT_451(config-pmap-c)#monitor parameters
UUT_451(config-pmap-c-mparam)#history 6 <----------- Error message will show
up
if previous history value is different
UUT_451(config-pmap-c-mparam)#interval duration 7 <----- Error message will
show up if previous interval duration is different
UUT_451(config-pmap-c-mparam)#react 102 mrv <-------- Error message will show
up if this react was not configured before or if the subsequent command
changes
the threshold value of the already-configured react.
```

Conditions:

1. This symptom is seen when configuring an inline service policy for the performance monitor on the Cisco ASR platform.
2. This symptom is seen when modifying monitor parameters of a noninline service policy for performance monitor on a Cisco ASR platform.

Workaround:

1. To configure the inline service policy, always specify all monitor parameters first and put the **flow monitor** *monitor name* command as the last command in the configuration.
2. To change monitor parameters, remove the service-policy by using the **no service-policy** command, make your changes, and then reattach the service-policy.

The above configuration restrictions do not apply if the enclosing policy-map is not attached to any interface. Also, the changes do not apply if you specify an “empty” flow monitor, for example a flow monitor without an enclosing valid flow record.

- 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 the configuration (the router will not be able to use warm reboot feature).

- CSCtu02543

  Symptoms: The assigned address for an EzVPN client is not freed up after a disconnect.

Conditions: This symptom is observed if there is another L2L tunnel terminating on the same interface of the EzVPN server.

Workaround: There is no workaround.

- CSCtu08373

  Symptoms: The router crashes at various decodes including fw_dp_base_process_pregen and cce_add_super_7_tuple_db_entry_common.

  Conditions: This symptom occurs when the Cisco IOS firewall is configured and traffic is flowing through the router.

  Workaround: There is no workaround.

- CSCtw65575

  Symptoms: The router may unexpectedly reload when OSPFv3 MIB is polled via SNMP.

  Conditions: This symptom occurs when OSPFv3 is configured with area ranges whose prefix length is /128. A router with no area ranges is not vulnerable.

  Workaround: Configure area ranges to have a smaller prefix length (that is, in the range of /0 to /127).

- CSCtw89123

  Symptoms: A router may crash after configuring “ppp fragment delay” under the multilink interface.

  Conditions: This symptom is observed when “ppp fragment delay” + policy-map is configured on a multilink interface and traffic passes through the HWIC-1ADSL card.

  Workaround: Increase the multilink fragment delay or remove QOS under the multilink interface.

- 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.

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCtx56183

  Symptoms: The router crashes due to block overrun:

```
%SYS-3-OVERRUN: Block overrun at 49156754 (red zone 66616365)
-Traceback= 42806C04z 42809B20z 42809D14z 427AD988z 427AD96Cz
.
.
%SYS-6-BLKINFO: Corrupted redzone blk 49156754....
.
%SYS-6-MEMDUMP: 0x49156754: 0xAB1234CD 0x12A0000 0x12C 0x44395148
%SYS-6-MEMDUMP: 0x49156764: 0x419B243C 0x49157154 0x49156658 0x800004E8
%SYS-6-MEMDUMP: 0x49156774: 0x1 0x0 0x1000133 0x47D7699C
```

  Conditions: This symptom occurs when Websense URL filtering is enabled and long URLs have been accessed.

  Workaround 1: Disable URL filtering.

  Workaround 2: Do not invoke long URLs.

- CSCtx75190

  Symptoms: In a multihomed setup, set up the traffic as explained in the DDTS. Once end-to-end traffic flows fine, do a RP switchover on ED1. Traffic from Ixia 3 to Ixia 1 and Ixia 3 to Ixia 2 on odd VLANs (ED1 is the AED for odd VLANs) is dropped with UnconfiguredMplsFia counters incrementing.

  Conditions: This symptom is observed when you do an RP switchover with a scaled OTV configuration in a multihomed setup.

  Workaround: There is no workaround.

- CSCty04384

  Symptoms: IMA-DSLAPP crashes when doing interoperability testing with third-party DSLAMs.

  Conditions: This symptom occurs when you change line rates on CO sides with various loop lengths.

  Workaround: There is no workaround.

- CSCty17288

  Symptoms: MIB walk returns a looping OID.

  Conditions: This symptom is observed when a media monitoring policy is configured.

  Workaround: Walk around CiscoMgmt.9999.

- CSCty44654

  Symptoms: The router crashes when trying to test the MVPN6 functionality.

  Conditions: This symptom is observed with the following conditions:

  - Configure the router to test the MVPN6 functionality.
  - Delete the VRF associated with the interface in the MVPN6 test configuration.

  Workaround: There is no workaround.

- CSCty57476

  Symptoms: The BGP GSHUT feature needs to add support for the AA:NN format for community.

  Conditions: This symptom is observed when support is added for the AA:NN format for community when using the BGP GSHUT feature.

  Workaround: The <1-4294967295> community number can be used instead of the AA:NN format.

- CSCty57856

  Symptoms: The Standby router crashes for an SRTP call on Active.

  Conditions: This symptom occurs intermittently. This issue is seen due to a transient scenario, where unstable data from Active is checkpointed on Standby.

  Workaround: There is no workaround.

- CSCty74859

  Symptoms: Memory leaks on the active RP and while the standby RP is coming up.

  Conditions: This symptom is observed when ISG sessions are coming up on an HA setup.

  Workaround: There is no workaround.

- 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.

- CSCtz55979

  Symptoms: The router crashes.

  Conditions: This symptom occurs when you configure CFM, SCE over MPLS, VPLS, or G.8032 services while running SNMP polling.

  Workaround: There is no workaround.

- CSCtz74540

  Symptoms: In a VSS system, the old Active Supervisor hangs after a mistral error interrupt occurs on the SP.

  Conditions: This symptom occurs on a VSS system, after a mistral hardware error (such as a parity error) occurs on the SP of the router. There is no issue if the error occurs on the RP.

  Workaround: There is no workaround. The switch with the old Active Supervisor must be power cycled.

- CSCtz83221

  Symptoms: Active or standby route processor crashes.

  Conditions: This symptom can be seen during the configuration or removal of ATM virtual circuits.

  Workaround: There is no workaround.

- CSCua01641

  Symptoms: The router's NAS-IP address contained in the RADIUS accounting-on packet is 0.0.0.0:

```
RADIUS:  Acct-Session-Id     [44]  10  "00000001"
RADIUS:  Acct-Status-Type    [40]  6   Accounting-On
        [7]
RADIUS:  NAS-IP-Address      [4]   6   0.0.0.0

 RADIUS:  Acct-Delay-Time     [41]  6   0
```

  Conditions: This symptom occurs when you restart the router.

  Workaround: There is no workaround.

- 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 the case of master switchover, synchronization between master and members is disrupted. This issue is seen only for IPv6 multicast routing. The issue is observed with a 9-member stack and either during the first or second master switchover. No issues are seen for IPv4 multicast routing.

  Workaround: This issue has been tested with a 5-member stack, and no issues are seen. It is recommended to enable IPv6 multicast routing when there is deployment with low members in a stack.

- CSCua24676

  Symptoms: The VRF to the global packet's length is corrupted by -1.

  Conditions: This symptom occurs when the next-hop in the VRF is global and recursive going out labeled. This issue is seen from Cisco IOS Release 15.0(1)S3a onwards, but is not seen in Cisco IOS Release 15.0(1)S2.

  Workaround: Use the next-hop interface IP instead of the recursive next-hop.

- CSCua31934

  Symptoms: A crash is seen at __be_address_is_unspecified.

  Conditions: This symptom is observed with the following conditions:

  1. It occurs one out of three times and it is a timing issue.
  2. DMVPN tunnel setup between Cisco 2901 as spoke and Cisco ASR 1000 as hub.
  3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  4. It can occur with v6 traffic alone.
  5. If you remove the tunnel interface on the Cisco ASR and add it again using **conf replace nvram:startup-config** the crash will occur.

  Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua37873

  Symptoms: The MCAST traffic drops for several seconds when the VSL link comes back up (control traffic).

  Conditions: This symptom occurs under the following conditions:

  - Around 2.5 minutes after SSO with 20000 mroutes.
  - When the Intranet is used.
  - When 100 mVRFs are defined.

  Workaround: Decrease the total number of mroutes to 10000.

- CSCua42104

  Symptoms: Malformed RTCP packets are observed.

  Conditions: This symptom occurs when DTMF interworking is enabled or SRTP/SRTCP is in use.

  Workaround: Disable DTMF interworking if not required for the call.

- CSCua47056

  Symptoms: The Cisco Catalyst 6000 crashes after the removal of the supervisor module from active VSS with the following traceback:

  ```
  0x41048F64 ---> ospf_rcv_dbd+F48
  0x41041FE8 ---> ospf_router+548
  0x4166C0B0 ---> r4k_process_dispatch+14
  0x4166C09C ---> r4k_process_dispatch
  ```

  Conditions: This symptom occurs when the following reproduction procedure is performed: NSF is disabled including helper using the below given commands:

  ```
  router ospf <AS>
  no nsf
  nsf cisco helper disable
  ```

  Adjacency flapped.

  NSF enabled again.

  Performed switchover.

  Workaround: Avoid the reproduction procedure in the production. Neighbors should see the router configured for “nsf cisco” as OOB resync capable:

  ```
  Router#sh ip ospf nei <interface> detail
  ...
      LLS Options is 0x1 (LR)   <-- LR bit means OOB resync capability
  ...
  ```

  If the router is configured for the “nsf cisco”, but the neighbor does not see LR bit set for the router with “nsf cisco”, flap the adjacency, and OOB resync capability will be renegotiated.

- CSCua47495

  Symptoms: The nine-member stack of the Cisco Catalyst 3750 gets into a low memory condition.

  Conditions: This symptom occurs with a default configuration on bootup.

  Workaround: There is no workaround.

- CSCua50697

  Symptoms: After unplugging and reconnecting a T1 cable, the T1 controller remains down or report continuous errors. After a router reload, the T1 controller remains up until the cable is disconnected again.

  Conditions: This symptom affects only the following cards: HWIC-xCE1T1-PRI, NM-8CE1T1-PRI, VWIC3-xMFT-T1/E1, and GRWIC-xCE1T1-PRI. Also, the T1 signal must be somewhat out-of-specification according to T1.403 standards.

  Workaround 1: Reload the router with the T1 cable plugged in.

  Workaround 2:

  1. Upgrade to a fixed-in Cisco IOS version.
  2. Issue the following commands (hidden, so tab complete will not work):

     ```
     enable
     config t
     controller <t1/e1> <slot/subslot/port> ! ( example: controller t1 0/0/0 )
     hwic_t1e1 equalize
     ```

  3) Shut/no shut the T1 controller, or reload the router to allow the CLI to take effect.

- CSCua61201

  Symptoms: Unexpected reload with BFD configured.

  Conditions: When a device is configured with BFD it may experience unexpected reloads.

  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.

- 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.

- CSCua75781

  Symptoms: CME reloads for E911 call ELIN translation for incoming FXS/FXO trunk.

  Conditions: This symptom is observed from Cisco IOS interim Release 15.3(0.2)T.

Workaround: There is no workaround.

- CSCua78782

  Symptoms: Authentication of EzVPN fails.

  Conditions: This symptom is observed with BR-->ISP-->HQ.

  Workaround: There is no workaround.

- CSCua82947

  Symptoms: Encapsulation for CFM messages may not be correct after the service instance encapsulation is changed. The “IOS-FMAN-EAOM-ERR” message may be observed.

  Conditions: This symptom occurs on an Ethernet CFM configured on a bridge-domain or xconnect service instance.

  Workaround: There is no workaround.

- CSCua94334

  Symptoms: Hung calls are seen on CME. Hung calls seen in “show call active voice brief” are as follows:

```
1502 : 26 36329310ms.1 +-1 pid:1 Answer XXXYYY4835 connected
dur 00:00:00 tx:0/0 rx:0/0
IP 0.0.0.0:0 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8
pre-ietf TextRelay: off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
```

  Conditions: This symptom is observed when an inbound H225 call setup request to a CME gateway results in a hung call if a release complete is received while still in alerting state. This issue occurs only when the shared line is configured on the phone and the shared line is not registered.

  Workaround: Remove the shared line or register the shared line.

- 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.

- 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.

- CSCub04982

  Symptoms: In an IPFRR configuration, a traceback is seen about changing the FRR primary OCE where the new OCE has a different interface and next-hop, which blocks such a linkage.

  Conditions: This symptom occurs while changing the FRR primary OCE interface to a new OCE with a different interface.

  Workaround: There is no workaround.

- CSCub14044

  Symptoms: A crash with traceback is seen, and all calls are dropped.

  Conditions: This symptom is observed under all conditions.

  Workaround: There is no known workaround. The gateway crashes, and the soak time appears to be six weeks.

- CSCub14145

  Symptoms: A Cisco ISR-G2 with VPN-ISM logs output similar to:

  ```
  !! Cannot find ISM-VPN counters struct for flowid: 0x44000084
  ```

  Conditions: This symptom is observed when using a VPN-ISM in an IPsec deployment with images from the Cisco IOS 15.2 train.

  Workaround: There is no workaround.

  Further Problem Description: The issue is cosmetic in nature while the VPN-ISM is queried for counters (for example, **show** commands).

- CSCub15402

  Symptoms: A VRF cannot be deleted. The following error message is displayed:

  ```
  error message "% Deletion of VRF VPNA in progress; wait for it to complete".
  ```

  Conditions: This symptom occurs after having previously issued “sh ip cef vrf * sum”.

  Workaround: There is no workaround. Reboot is required to remove the VRF.

- CSCub17584

  Symptoms: Cisco IOSD crashes seen with 1K MVPN sessions. (When the sessions are cleared, all the IGMP joins are released, and then the sessions are brought up. When there are about 400 to 500 IGMP joins, the crash is seen.)

  Conditions: This symptom occurs while clearing the 1K MVPN sessions on LAC using “clear pppoe all”.

  Workaround: There is no workaround.

- CSCub17971

  Symptoms: There is no re-registration after switching from HW to SW crypto engine.

  Conditions: This symptom is observed after switching from HW to SW crypto engine.

  Workaround: There is no workaround.

- CSCub19185

  Symptoms: Path confirmation fails for a SIP-SIP call with IPV6 enabled.

  Conditions: This symptom occurs when UUTs are running Cisco IOS Release 15.2(2)T1.5.

  Workaround: There is no workaround.

- CSCub26079

  Symptoms: Service policies are not getting applied on ATM interface.

  Conditions: This symptom is observed when client is configured with “ppp chap hostname peer” and a PPPOA session is established. Policies 7up and sprite are installed on the interface of UUT. Later, the client “ppp chap hostname Rate” is configured, and that time, policies are downloaded from radius, which have not replaced previous policies 7up and sprite.

  Workaround: There is no workaround.

- CSCub30381

  Symptoms: The router crashes very frequently.

  Conditions: This symptom is observed with a router configured with X25 and any dynamic routing protocol.

  Workaround: Use static routing instead of dynamic routing.

- CSCub34534

  Symptoms: A basic call between two SIP phones over SIP trunk (KPML-enabled) fails. Conditions: This symptom is observed with Cisco ISR G2 platforms.

  Workaround: There is no workaround

- CSCub36403

  Symptoms: Standby reloads due to no switchport.

  Conditions: This symptom occurs when you configure a port as “no switchport”. No IP configuration needed. Set the “tftp source interface <>”. Now, defaulting the interface causes this issue.

  Workaround: There is no workaround.

- CSCub38559

  Symptoms: When static recursive routes are used in an MVPNv6 environment, multicast traffic loss can occur due to failure to determine the correct RPF interface for a multicast source or rendezvous point.

  Conditions: This symptom occurs if a static route to an IPv6 address at a remote site (remote side of a VPN cloud) resolves via a BGP route, resulting in a failure to install the required MDT alternate next-hop in the recursively referenced BGP route.

  Workaround: Executing “show ipv6 rpf vrf X <address>” for any address within the recursively referenced BGP prefix range will cause installation of the required alternate next-hop.

- CSCub42181

  Symptoms: The router crashes continuously after a normal reboot due to power or some other reason.

```
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M4,
RELEASE SOFTWARE (fc1)
 uptime is 4 days, 11 hours, 38 minutes
System returned to ROM by error - a Software forced crash, PC 0x88D26F0 at
07:42:45 UTC Sat May 5 2012
System restarted at 07:43:55 UTC Sat May 5 2012
System image file is "flash:c3900-universalk9-mz .SPA.150-1.M4.bin" ;
Last reload type: Normal Reload

---------------------------
```

  Generated Traceback:

  Pre Hardware Replacement Crashinfo:

```
-----------------------------------
#more flash0:crashinfo_20120519-165015-UTC

-----------------
```

  Traceback Decode:

```
-----------------

tshakil@last-call-2% rsym c3900-universalk9-mz.150-1.M4.symbols.gz
Uncompressing and reading c3900-universalk9-mz.150-1.M4.symbols.gz via
/router/bin/zcat
c3900-universalk9-mz.150-1.M4.symbols.gz read in
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c

0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
Enter hex value:

-------------------------------
```

Crash File Post Installation:

```
-----------------------------

#more flash0:crashinfo_20120519-185725-UTC

-----------------
```

Traceback Decode:

```
-----------------

Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
-------------------------------------------------
```

Conditions: This symptom is observed with the following conditions:

- MGCP gateway.
- Take out all the modules from the router.
- Put the modules one by one.
- Apply the configuration.
- The router is stable.

The lab test can be recreated as follows:

1. 1) Disable auto-configuration, that is, “no ccm-manager config” .

2. Reload the gateway.
3. Enable the CCM manager configuration and the router does not crash.

Workaround 1: Bypass the start-up configuration and log in via ROMmon without any configuration. Add the configuration one by one. Once the configuration is added, save the configuration and reload the gateway.

Workaround 2: Shut down the router and add the cards one by one in slots 0, 1, 2, 3, and 4. The device is stable until the third slot is inserted and brought up. As soon the router is powered on, after adding the fourth slot, the crash starts. Shut down the router and remove the card in slot 4 (EVM-HD-8FXS/DID). Bring the device up without the card in slot 4 (EVM-HD-8FXS/DID). Remove the "mgcp" and "ccm-manager fallback-mgcp" configuration from the device because the console log is displaying the "Call Manager backhaul registration failed" error message. Shut down the router and add the card which was removed. Bring up the router. Readd the **ccm-manager fallback-mgcp** command and do a "no mgcp/mgcp". The router becomes stable.

Workaround 3: Remove the **ccm-manager config** command by issuing "no ccm-manager config", which tears down the connection from the call manager to the MGCP gateway. The gateway will not download the configuration from the call agent at the time of startup. Reload the router. Once the router is back and stable, readd the command.

- CSCub44898

  Symptoms: Stale scansafe sessions are seen on the router. They do not get cleared even with the **clear content-scan sessions *** command.

  Conditions: This symptom occurs when one of the end points (client or server) does not properly close the connection. In TCP terms, when one end does not send an ACK to the FIN request sent by the other end in L4F UNPROXIED state.

  Workaround: There is no workaround. The router needs to be rebooted to clear the stale sessions.

- CSCub45054

  Symptoms: OQD drop counters increment on the mGRE tunnel even though there are no drops.

  Conditions: This symptom is observed with an mGRE tunnel when multicast traffic is sent over the tunnel. This issue is seen when EIGRP or OSPF is configured on the tunnel.

  Workaround: There is no workaround.

- CSCub52825

  Symptoms: The negotiated global IPv6 remains intact on the Dialer interface.

  Conditions: This symptom is observed when the physical interface goes down.

  Workaround: Remove the global IPv6 address manually from the Dialer interface.

- CSCub52943

  Symptoms: When executing Media Forking with midcall codec change, memory leaks are found in Cisco ASR for CCSIP_SPI_CONTROL. After decoding, the memory leak is found to be for the function is_x_participant_sips() as it is not releasing the memory after allocated with some memory. This seems to be a side effect of one of the DDTS that was committed to Cisco IOS Release 15.3M&T (CSCtz96408).

  Conditions: This symptom occurs when executing Media Forking with midcall codec change.

  Workaround: The fix is done and is committed to Cisco IOS Release 15.3M&T.

- CSCub54872

  Symptoms: A /32 prefix applied to an interface (for example, a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.

Conditions: This 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.

- CSCub55297

  Symptoms: The CEM interface (Serial Interface Network Modules - NM-CEM-4SER and NM-CEM-4TE1) does not come up with the latest Cisco IOS Release 15.3(1)T image.

  Conditions: This symptom is observed with Cisco IOS Release 15.3(1)T.

  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

- CSCub56064

  Symptoms: Ping fails after doing EZVPN client connect if CEF is enabled.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(0.8)T image. This issue is seen only for a specific topology, where the in/out interface is the same.

  Workaround: There is no workaround.

- CSCub59493

  Symptoms: The CPU remains at 100% after the SNMPv 2c walk even after 5 minutes.

  Conditions: This symptom occurs when an SNMP walk is done on mplsLsrStdMIB.

  Workaround: There is no workaround.

- CSCub61009

  Symptoms: Spurious errors are observed on the Cisco AS5400.

  Conditions: This symptom is observed with the Cisco AS5400.

  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 6.8/6.5:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C

  CVE ID CVE-2012-5422 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

- CSCub61795

  Symptoms: The log fills with SYS-2-BADSHARE messages, leading to a crash.

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=69AD4440, count=0
  ```

```
-Traceback= 601E887Cz 601E50B4z 601E56C0z 602D24CCz 60F38F04z 6065B628z
 Invalid magic number in receive buffer (0x0)
```

Conditions: This symptom occurs with a large amount of traffic passing through an ATM interface. This issue might be specific to an ATM interface using the CX27470 ATMOC3 driver as seen in the **show interface** command output. The ATM module that the issue was originally seen on was a NM-1A-OC3-POM. QOS might be needed to trigger the issue.

Workaround: A possible but unconfirmed workaround is to disable QOS on the interface.

- CSCub66367

  Symptoms: When using HWIC-2SHDSL with “ppp mulitlink fragment” configured, there is some packet loss when pings are sourced from a PC. But, when pings are sourced from the router, there is no ping loss. When “ppp mulitlink fragment” is not configured, no ping loss is experienced even when pinging from the PC.

  Conditions: This symptom occurs when “ppp mulitlink fragment” is configured.

  Workaround: There is no workaround.

- 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”.

- CSCub71981

  Symptoms: The **show voice register pool on-hold brief** command displays the same number (for both phone number and remote number) when both local and remote phone are put on on-hold.

  Conditions: This symptom is observed when with Cisco IOS Release 15.3(8)T.

  Workaround: There is no workaround.

- CSCub74272

  Symptoms: Intermittently during Phase II rekey, after new SPIs are negotiated and inserted into SPD, old SPIs are removed and then the VTI tunnel line protocol goes down.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T, with VTI over GRE.

  Workaround: There is no workaround.

- CSCub78299

  Symptoms: Ping fails from host1 (192.168.1.2) to host2 (192.168.4.2).

  Conditions: This symptom occurs when Suite-B is configured on IPsec sa.

  Workaround: There is no workaround.

- CSCub79318

  Symptoms: Codec changes spontaneously during midsession without a RE-INVITE.

  Conditions: This symptom occurs with the following conditions:

  - Fax passthrough is configured.
  - Codec negotiated is G711alaw, and changes to G729.

  Workaround: There is no workaround.

- CSCub80386

  Symptoms: The following interface configuration should be used:

  ```
  interface Ethernet2/1
  description lanethernet1
  ipv6 enable
  ospfv3 100 network manet
  ospfv3 100 ipv6 area 0
  ```

  Dead interval is calculated according to network type; in this case, it is 120s. Issue the **no ospfv3 dead-interval** command on dead interval. Dead interval is set to the default of 40s instead of 120s, which is correct for manet or P2MP interface types.

  Conditions: This symptom is an OSPFv3-specific issue (see the configuration example).

  Workaround: Configure dead interval explicitly or reapply the network command.

- CSCub80654

  Symptoms: Randomly, there is no audio if a call comes from the following call flow using G729:

  ```
  IP Phone -- CUCM -- ICT GK Controlled -- GK -- CME 9.1 -- Phone A and B
  ```

  If one of the phones in CME tries to GPickup the call randomly, it will have no audio. When this happens, if you check the codec directly in the phone, it is G711. However, when it works, it is G729. Everything is configured for G729. Even if you hard code the phone in CME to use G729, this issue will occur. This issue does not occur in CME 7.1.

  Conditions: This symptom occurs if a call comes from GK as G729 and CME 9.1 is being used.

  Workaround: Use CME 7.1 or enable fast start in CUCM Trunk by enabling the following check boxes:

  - Media Termination Point Required
  - Enable Outbound FastStart

- CSCub80710

  Symptoms: SSL handshake between Cisco VCS and the Cisco ASR fails if the Cisco ASR is running Cisco IOS XE Release 3.7S.

  Conditions: This symptom occurs in a working setup, if the Cisco ASR is upgraded to Cisco IOS XE Release 3.7S, then SSL handshake and subsequently SIP-TLS calls start to fail. If in the same setup, the Cisco ASR is downgraded back to Cisco IOS XE Release 3.5S or Cisco IOS XE Release 3.4.4S, then the calls work (without requiring any additional changes).

  Workaround: There is no workaround.

- CSCub82495

  Symptoms: Channel-group goes down with the HWIC-xCE1T1-PRI controller after reloading the router.

  Conditions: This symptom occurs when channel-group goes down after reload.

  Workaround: There is no workaround.

- CSCub85451

  Symptoms: When scansafe is enabled on the interface, latency may be seen. Some pages may not load at all or show severe latency if the SYN request sent by the ISR does not receive an appropriate SYN ACK response from the Scan Safe Tower.

  Conditions: This symptom occurs when scansafe is enabled on the interface. In this case, there was an ASA in the path that was doing sequence number randomization.

Workaround: Disable sequence number randomization on the firewall in the path before the ISR.

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-2012-4651 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

- CSCub86011

  Symptoms: The embedded event manager (EEM) is not available on the Cisco VG202/204.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T or later releases.

  Workaround: There is no workaround.

- CSCub88742

  Symptoms: A crash occurs due to NULL pointer access in a BGP C-Route function.

  Conditions: This symptom is very timing-sensitive and will occur only in a specific sequence of runtime events in a specific timing instance. In this case, this issue is triggered in a scaled setup when "mpls mldp" is toggled after two SSOs and when each SSO takes a very long time to complete due to HA Bulk Sync failure in IP Multicast that has addresses separately.

  Workaround: There is no workaround.

- CSCub89144

  Symptoms: In a VTI scenario with HSRP stateless HA, the tunnel state on standby is up/up.

  Conditions: This symptom occurs when HSRP is configured and there is no SSO configuration.

  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.

- 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.

- CSCub93496

  Symptoms: One-way video from CTS-1000 to TS-7010 is seen in the following topology:

  ```
  CTS-1000 (v1.9.1) >>> CUCM 8.6.2aSU2 >>> CUCM 9.0 >>> CUBE 15.1.2T (2811) >>>
  CUBE 15.1.4M4 (2951) >>> CUCM9.0 >>> VCS X7.1 >>> TS-7010 2.2
  ```

  Conditions: This symptom occurs when SDP Passthru mode on CUBE is used.

  Workaround: RTP payload types 96/97, which are associated with fax/faxack need to be remapped to some other unused values.

- CSCub96618

  Symptoms: An error message is seen on standby.

  Conditions: This symptom is observed with tunnel configurations.

  Workaround: There is no workaround.

- CSCub98623

  Symptoms: The **show int** command output displays the input queue size as bigger the 0, and never goes down. Shut/no shut does not help as well.

  Conditions: This symptom is observed with the following conditions:

  – A Cisco IOS router actions as XOT.

  – The XOT Server becomes not reachable for sometime while the x25 client is attempting to send traffic.

  – Cisco IOS Release 12.4(24)T7, Cisco IOS Release 15.1M ,or later releases.

  Workaround: Increase the input hold queue size from default 75 to max. Monitor it periodically manually or by script and perform a planed reload when the queue size is close to max.

- CSCuc07984

  Symptoms: The Cisco 819 router serial interface does not interoperate with modems such as Adtran, Aethra,and Pardayn.

  Conditions: This symptom occurs on the serial interface on the Cisco 819 series router while connecting to some specific types of modems.

  Workaround: There is no workaround.

- CSCuc08061

  Symptoms: IPv6 DMVPN spoke fails to rebuild tunnels with hubs.

  Conditions: This symptom occurs when the tunnel interface on the spoke is removed and reapplied again.

  Workaround: Reboot the spoke.

- CSCuc08895

  Symptoms: A switching failure occurs after applying the CEM configuration.

  Conditions: This symptom occurs when there is a PW redundancy and the primary VC is down. Reapply the configuration.

```
config term
controller e1 0/7
cem-group 0 unframed
end

config term
interface cem 0/7
cem 0
no xconnect 180.0.0.201 17 encap mpls
end
```

  Workaround: Remove the xconnect configuration. Potentially, wait for 20 minutes in the worst case for “sh mpls l2 pwid” to age out labels.

- CSCuc09483

  Symptoms: Under certain conditions, running a TCL script on the box may cause software traceback and reload of the affected device.

Conditions: This symptom is observed when the Privilege 15 user may run TCL commands that may lead to an affected device reloading.

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 3.8/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:S/C:N/I:N/A:C/E:F/RL:U/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: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc10588

  Symptoms: The router crashes.

  Conditions: This symptom occurs when the normalizer engine is running with the traffic being sent.

  Workaround: There is no workaround.

- CSCuc12685

  Symptoms: Address Error exception is observed with ccTDUtilValidateDataInstance.

  Conditions: This symptom is observed with ccTDUtilValidateDataInstance.

  Workaround: There is no workaround.

- CSCuc13992

  Symptoms: The Cisco IOSd process crashes due to a segmentation fault in the PPP process:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = PPP Events
  ```

  The root cause for the PPP process crash is wrong IPCP option processing inside PPP control packets.

  Conditions: This symptom occurs when the BRAS functionality is configured, which includes ISG and PPPoE session termination.

  Workaround: There is no workaround.

- CSCuc14088

  Symptoms: The default class is not being exported with the class option template.

  Conditions: This symptom occurs when class-default is not exported when typing the option c3pl-class-table under the flow exporter.

  Workaround: 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.

  Workaround 1: Disable CEF.

  Workaround 2: Do not configure "ip traffic-export" in the crypto map interface.

  Workaround 3: Disable ISM using "no cry engine slot 0". Then, the onboard engine will be used.

- CSCuc15695

  Symptoms: The counters are not polling the correct stats.

  Conditions: This symptom was first observed on the ATM interfere, but it is not particular to the ATM as this issue was reproduced on the Gigabit Ethernet interface as well.

  Workaround: There is no workaround.

- CSCuc16172

  Symptoms: When the reset button is pushed on a Cisco C881W-A-K9 router, the start-up configuration is automatically backed up as “startup.backup.xxx” and stored in the flash.

  Conditions: This symptom occurs when a xxx.cfg file is present on the flash and the push button is pressed. The Cisco C881W-A-K9 Router boots up with the xxx.cfg file present on the flash, but also backs up the start-up configuration as “startup.backup.xxx” and stores it on the flash.

  Workaround: There is no workaround.

- 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.

  Workaround: There is no workaround.

  Further Problem Description: So far, this issue is only seen in the FFM performance test script.

- CSCuc19800

  Symptoms: The router crashes.

  Conditions: This symptom occurs when the **no switchport** command is issued under the UCSE x/1 interface.

  Workaround: There is no workaround.

- CSCuc19862

  Symptoms: Traceback and CPU hog is seen due to spurious memory access when Flexible NetFlow (FNF) is enabled.

  Conditions: This symptom is seen when enabling FNF.

  Workaround: Use classic netflow or configure FNF on the tunnel template interface (preferred).

  Note: The first option of using classic netflow is not available on some platforms which only support FNF. Notably, these are the Cisco Catalyst 6000, the Cisco Catalyst 6500 Series Supervisor Engine 2T, and the Cisco Catalyst 4000 with K10.

- CSCuc24937

  Symptoms: The voice gateway router is configured as a CME for handling ephone reloads due to spurious memory access.

  Conditions: This symptom occurs as the voice gateway router is capable of handling ephones. Reload is very specific to ephone handling.

  Workaround: There is no workaround.

- CSCuc28931

  Symptoms: The router crashes due to high CPU and lack of memory.

  Conditions: This symptom occurs when using a local connect between an EFP with encap dot1q and an EFP with encap untagged.

Workaround: There is no workaround.

- CSCuc29310

  Symptoms: TD probes in fast mode are gone when the link flaps (not PfR external interfaces).

  Conditions: This symptom is observed with TD, fast mode, and link flap, which cause SAF session flap.

  Workaround: Issue “clear pfr mas tr”.

- CSCuc30630

  Symptoms: An update to the Cisco IOS-IPS signature package may cause the router to crash in some very rare scenarios, when signature scanning and signature build happens simultaneously.

  Conditions: This symptom occurs on a Cisco 2911 ISR G2 router running Cisco IOS Release 15.2(4)M1.

  Workaround: There is no workaround.

- CSCuc31534

  Symptoms: With a primary PW in the down state, if the Xconnect redundancy configuration is removed and added, then switching may remain down and the VC goes down.

  Conditions: This symptom is observed with the following conditions:

  1. The platform supports hot standby (Cisco ASR 903/Cisco 7600/Cisco ASR 901).
  2. PW redundancy with primary down.
  3. Configuration removed + added or added afresh.

  Workaround: Fix the primary PW and then remove/add the configuration.

- CSCuc31725

  Symptoms: CUBE fails to resolve the configured DNS through A query when the SRV query fails.

  Conditions: This symptom occurs when running Cisco IOS Release 15.3(0.11)T.

  Workaround: Use DNS SRV records for SIP servers.

- CSCuc33328

  Symptoms: Memory leaks are seen in the statistics.

  Conditions: This symptom occurs when the probe is executed and statistics are updated.

  Workaround: There is no workaround.

- CSCuc36469

  Symptoms: A crash is observed when removing the **crypto call admission limit ike in-negotiation-sa** *value* configuration and clear crypto sessions, which triggers a connection from all the clients burdening the server and forcing it to crash within seconds.

  Conditions: This symptom occurs only when 150 connections simultaneously try to establish connection with the head-end EzVPN server.

  Workaround: Configure **crypto call admission limit ike in-negotiation- sa** *20* when scaling to 150 tunnels.

- CSCuc37047

  Symptoms: VSS crashes on reconfiguring “ipv6 unicast-forwarding” multiple times.

  Conditions: This symptom occurs when CTS is configured on an interface and “ipv6 unicast” is toggled multiple times.

Workaround: There is no workaround.

- CSCuc39963

  Symptoms: Spurious memory access/crash is seen at mdb_tree_classify.

  Conditions: This symptom occurs when the egress QoS policy is configured.

  Workaround: There is no workaround.

- CSCuc40448

  Symptoms: No-way audio is observed on hair-pinned calls back from CUBE to SIP Provider.

  The call flow is as follows:

  ```
  PSTN caller --Verizon---(sip)---ASR CUBE---(sip)---CUSP---(sip)---Genesis ( SIP
  Refer sent to transfer back to Verizon) -- CUSP - CUBE - Verizon -- PSTN
  ```

  Conditions: This symptom is observed only after upgrading to Cisco IOS Release 15.2(2)S.

  Workaround: Modify the diversion header on the transfer leg invite, so Verizon handles the call differently.

- CSCuc41531

  Symptoms: Forwarding loop is observed for some PfR-controlled traffic.

  Conditions: This symptom is observed with the following conditions:

  - Traffic Classes (TCs) are controlled via PBR.
  - The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class ...** command (this fixes the issue until the next occurrence).

- CSCuc41596

  Symptoms: Connection to the remote server fails with “domain name” when port-forward is configured with a VRF.

  Conditions: This symptom occurs when the VRF is configured on the router and the backend server is opened over HTTP using port-forward. The link opens when accessing directly using IP, but fails when a domain name is used after configuring a domain server.

  Workaround: Configure the IP address instead of the domain name.

- 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 DoS from the interface input queue wedge condition while trying to process certain RTCP packets during media negotiation using SIP.

  Conditions: This symptom occurs when Cisco IOS CUBE may experience an input queue wedge condition on an interface configured for media negotiation using SIP when a 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

- CSCuc43943

  Symptoms: A Cisco ASR 1000 hub on dual-hubs DMVPN crashes. This issue is only seen in Cisco IOS XE Release 3.9S.

  Conditions: This symptom is observed with shut/no shut of the tunnel interface.

  Workaround: There is no workaround.

- CSCuc44438

  Symptoms: There is a memory corruption issue with loading NBAR protocol pack.

  Conditions: This symptom occurs when an NBAR protocol pack is loaded into the router using the **ip nbar protocol-pack** command.

  Workaround: There is no workaround.

- CSCuc44629

  Symptoms: The switch/router crashes while processing NTP.

  Conditions: This symptom occurs if NTP is configured using DNS, along with the source interface. For example:

  ```
  config# ntp server <dns> source <interface>
  ```

  Workaround 1: config# ntp server <dns>

  Workaround 2: config# ntp server <ip>

  Workaround 3: config# ntp server <ip> source <interface>

  For workarounds 1 and 2, the device automatically selects the source interface. For workarounds 2 and 3, resolve the DNS and use the corresponding IP address for that DNS. For example:

  ```
  Router# ping <dns>
  ```

  The above command gives the IP address for DNS. Use that IP address to configure the NTP server.

- CSCuc45115

  Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.

  Conditions: This symptom is observed in the case where there are two Overlay addresses of different Addr Family on the same NBMA (such as IPv4 and IPv6 over Ipv4). This issue is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

  Workaround: There is no known workaround.

- CSCuc45528

  Symptoms: Incremental leaks are seen at :__be_nhrp_recv_error_indication.

  Conditions: This symptom occurs when the NHRP error indication is received on the box. This issue is seen only if CSCub93048 is already present in the image. CSCub93048 is available from Cisco IOS Release 15.3M&T onwards.

  Workaround: There is no workaround.

- CSCuc46087

  Symptoms: CUBE does not send a response to an early dialog UPDATE in a glare scenario.

  Conditions: This symptom occurs when CUBE receives an early dialog UPDATE when it sends 200OK to INVITE and expects ACK.

  Workaround: There is no workaround.

- CSCuc46827

  Symptoms: There is an RP crash at __be_NetworkInterface_setAddressIDL.

  Conditions: This symptom occurs when an interface IP address is removed through OnePk API.

  Workaround: Use CLI to resolve the issue.

- CSCuc47356

  Symptoms: Static routes are not getting removed.

  Conditions: This symptom is observed with Smap - Smap. Removal of CLI does not remove the static route.

  Workaround: Remove the ACL before removing the SA.

- CSCuc47399

  Symptoms: IKEv2 STOP Accounting records show wrong counters for packets/octets, when the sessions are locally cleared using “clear crypto sa” or “clear crypto session” on the Cisco ASR 1000.

  Conditions: This symptom is observed with latest Cisco IOS XE Release 3.8S images when IKEV2-Accounting is enabled. This issue is easily reproducible with a single session, and may be service impacting as STOP Accounting records are usually used for billing purposes.

  Workaround: The STOP records reflect the right counters when the disconnect is through the remote-end.

- CSCuc47675

  Symptoms: Traffic blackhole when a single pair of 4-wire EFM bond connection is down on a Cisco 888E router.

  Conditions: This symptom is observed when connecting to a third-party vendor DSLAM from a Cisco 888E router.

  Workaround: There is no workaround.

- CSCuc48211

  Symptoms: Traffic from the Label Edge Router (LER) is dropped at the Label Switch Router (LSR) peer. LER is using a invalid/outdated label, unknown to LSR. This issue can be seen with a regular MPLS connection over a physical interface or with a connection over an MPLS TE tunnel interface. The root cause is that LER is using CEF long-path extension, installed to the prefix by a different routing protocol in the past.

```
TUNNEL-HEADEND/LER#show ip cef 172.25.0.1 internal
172.25.0.0/16, epoch 6, flags rib only nolabel, rib defined all labels, RIB[B],
refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00018000
   Broker: linked, distributed at 4th priority
   LFD: 172.25.0.0/16 0 local labels
        contains path extension list
  ifnums:
   TenGigabitEthernet1/0/0(31): 10.10.243.48
   Tunnel11(38)
```

```
  path 1F13EC1C, path list 1436FC80, share 1/1, type recursive, for IPv4
  recursive via 10.10.254.3[IPv4:Default], fib 21B2A5CC, 1 terminal fib,
v4:Default:10.10.254.3/32
    path 13A71668, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label 1683
    nexthop 10.10.243.48 TenGigabitEthernet1/0/0 label 1683, adjacency IP adj
out of TenGigabitEthernet1/0/0, addr 95.10.243.48 20BCED00
    path 13A745A8, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label 623
      MPLS long path extensions: MOI flags = 0x1 label 18
    nexthop 10.10.255.130 Tunnel11 label 18, adjacency IP midchain out of
Tunnel11 22923160
  long extension for path if Tunnel11 next hop 10.10.255.130:
    MPLS long path extensions: MOI flags = 0x1 label 18
  long extension for path if Tunnel22 next hop 10.10.255.129:
    MPLS long path extensions: MOI flags = 0x1 label 651
  output chain:
    loadinfo 212F8810, per-session, 2 choices, flags 0083, 4 locks
    flags: Per-session, for-rx-IPv4, 2buckets
    2 hash buckets
      < 0 > label 1683 TAG adj out of TenGigabitEthernet1/0/0, addr
10.10.243.48 20BDC860
      < 1 > label 18 TAG midchain out of Tunnel11 20C92B00 label implicit-null
TAG adj out of TenGigabitEthernet1/0/1, addr 10.10.243.50 20B21440
    Subblocks:
     None

TUNNEL-TAILEND/LSR# sh mpls forwarding-table labels 18
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
TUNNEL-TAILEND#
```

Conditions: This symptom occurs when the prefix is learned by both BGP and IGP, while BGP has lower Administrative Distance, pointing via the MPLS TE tunnel carrying MPLS. This issue is seen once the prefix is installed to RIB by IGP and then by BGP (Reload, BGP flap, etc.); then, the CEF will keep using the IGP/LDPs label without updating it in case of LDP label change.

Workaround: Issue the **clear ip route** *prefix mask* command.

- CSCuc49335

  Symptoms: An infinite loop is seen at tunnelInetConfigIfIndex.ipv6 while doing SNMP walk.

  Conditions: This symptom occurs when an SNMP walk is done on the Cisco ISRG2 router and the Cisco ASR 1000 router.

  Workaround: There is no workaround.

- CSCuc49364

  Symptoms: A discrepancy is seen between show profile flow and show metadata table.

  Conditions: This symptom is observed on SIP Re-invite.

  Workaround: There is no workaround.

- CSCuc50398

  Symptoms: The client is crashing while doing Telnet from host to server.

  Conditions: This symptom is observed with the following setup:

  ```
  host <---> client <---> mid-router <---> server
  ```

  It is crashing consistently due to memory overrun.

  Workaround: There is no workaround.

- CSCuc51692

  Symptoms: The router crashes while enabling L2TP debugs using the **debug l2vpn l2tp error | event** command.

  Conditions: This symptom always occurs on enabling the **debug l2vpn l2tp error | event** command.

  Workaround: The same debugs can be enabled using the alternate command **debug xcl2 error | event**.

- CSCuc54220

  Symptoms: The SVTI always-up feature is broken.

  Conditions: This symptom occurs in clear and rekey cases.

  Workaround: Use shut and no shut.

- CSCuc54300

  Symptoms: The following error message is seen during a system reboot/boot:

  ```
  "Notification timer Expired for RF Client: Redundancy Mode RF(5030)"
  ```

  Conditions: This symptom occurs during a system reboot/boot.

  Workaround: There is no workaround. This is a rare bug which needs a specific timing sequence to occur. The system reloads after this error. In most cases, the system will come up smoothly after a reload, else it will come up after one or two reloads.

- CSCuc55346

  Symptoms: SNMP MIB cbQosCMDropPkt and cbQosCMDropByte report 0.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)S1 and Cisco IOS Release 15.2. This issue is not seen with Cisco IOS Release SRE4.

  Workaround: Use SNMP MIB cbQosPoliceExceededPkt and cbQosPoliceExceededByte.

- 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).
  4. Configure IPv6 static route via the interface configured in item 3, (for example, IPv6 route 2001:192:14:1::/64 2001:192:44:1::1).
  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 symptom occurs 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.

- CSCuc59541

  Symptoms: Spoke fails to learn networks behind other spokes and EIGRP flapping occurs.

  Conditions: This symptom is observed with a FlexVPN spoke-to-spoke setup.

  Workaround: There is no workaround.

- CSCuc63531

  Symptoms: The following traceback may be displayed after performing Stateful Switchover:

  ```
  %SYS-2-NOBLOCK: may_suspend with blocking disabled.
  ```

  Conditions: This symptom is observed when Stateful Switchover is performed with the **template type pseudowire** command configured.

  Workaround: There is no workaround.

- CSCuc63884

  Symptoms: A router configured with HSRP and RF interdev may experience an NMI watchdog during reload after failover, as it transitions from a standby to an active state.

  ```
  SYS-2-INTSCHED 'sleep for' at level 6 -Process= "RF Interdev reload process", ipl= 6,
  pid= 316
  NMI Watchdog timeout!!: vector 2, PC = 0x219B3C
  ```

  Conditions: This symptom is observed with HSRP and interdev configured. HSRP failover is triggered by link failure if the configuration is being saved at the same time.

  Workaround: There is no workaround.

- CSCuc66122

  Symptoms: A crash occurs with the **show ip sla summary** command with the IP SLAs RTP-Based VoIP Operation.

  Conditions: This symptom occurs when the IP SLAs RTP-Based VoIP Operation is configured on the box.

  Workaround: Use the **show ip sla statistics** command to check the status and statistics of the IP SLAs RTP-Based VoIP Operation rather than **show ip sla summary** command, when the IP SLAs RTP-Based VoIP Operation is configured on the box.

- 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= 23B9EA7Cz 23BA1A44z 23BA1E24z 23B712B8z 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.

- CSCuc67687

  Symptoms: With a rare combination, and VRF-related RG configurations, the router may crash following the configuration commands.

  Conditions: This symptom is observed with the following configuration:

```
R1-13RU(config-if)#ip vrf forwarding b2b-vrf
% Interface GigabitEthernet0/1/0 IPv4 disabled and address(es) removed due to
enabling VRF b2b-vrf
% Interface GigabitEthernet0/1/0 virtual IP address <ip> removed due to VRF change
% Zone security Z1 is removed due to VRF config change on interface
GigabitEthernet0/1/0

R1-13RU(config-if)#ip address <ip> <mask>
R1-13RU(config-if)#zone-member security Z1
R1-13RU(config-if)#redundancy group 1 ip <ip> exc dec 50
```

  Workaround: There is no known workaround.

- CSCuc68743

  Symptoms: A crash occurs while running CME smoke regression.

  Conditions: This symptom is observed while running CME smoke regression.

  Workaround: There is no workaround.

- CSCuc69342

  Symptoms: About 10 minutes after CUBE boot, the router crashes with the following traceback:

```
-Traceback= 5B01805 46158ED 45F4F57 45BB19E 45BA1CF 451D6DC 4525549 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.

- CSCuc70310

  Symptoms: RRI routes are not installed in DMAP. “reverse-route” is a configuration in the DMAP. This prevents packets from being routed through the intended interface, and hence packet loss occurs.

Conditions: This symptom is observed when a simple reverse-route is configured in DMAP without any gateway options.

Workaround: There is no workaround.

- CSCuc71493

  Symptoms: Significant transaction time degradation is observed when an e-mail with attachment(s) is sent from the Windows 7 client using Outlook to a server running Outlook 2010 on the Windows 2008 server and the WAN latency is low, that is, ~12ms RTT.

  Conditions: This symptom is observed when the client is Windows 7 and data is being uploaded using the MAPI protocol and the connection is being optimized by WAAS-Express.

  Workaround: Disable WAAS-Express.

- CSCuc71706

  Symptoms: Execution of the **show run** command and other commands such as **copy run start** and **show access-list** cause the router to stop for a few minutes before completing.

  Conditions: This symptom is observed with Cisco ISR G2 routers. This issue is seen only with IPV6 configured and used.

  Workaround: There is no workaround.

- CSCuc72594

  The Cisco IOS Software implementation of the IP Service Level Agreement (IP SLA) feature contains a vulnerability in the validation of IP SLA packets 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. Mitigations for this vulnerability are available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ipsla

  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:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCuc73473

  Symptoms: The IPv6 default route is not redistributed in BGP(VRF).

  Conditions: This symptom occurs when the OSPFv3 “default-information originate always” is configured in the same VRF.

  Workaround: To clear the issue, enter “cle ip bg *”. To avoid the issue, remove “default-information originate always” from OSPFv3 in the respective VRF.

- CSCuc73677

  Symptoms: RSA keys are not generated correctly.

  Conditions: This symptom occurs when you first clear the RSA keys that are already generated on the router, and then generate the RSA keys.

  Workaround: There is no workaround.

- CSCuc76130

  Symptoms: IPsec SAs are not getting deleted even after removing ACL.

  Conditions: This symptom occurs when using the IPsec feature with Cisco IOS Release 15.3(0.18)T0.1.

  Workaround: There is no workaround.

- CSCuc76298

  Symptoms: In a Cisco ASR B2B HA setup, the new active router crashes at ccsip_send_ood_options_ping immediately after switchover with OOD OPTIONS enabled.

  Conditions: This crash is seen in the following scenario:

  – Standby router has OOD OPTIONS enabled either because it is present in the startup-configuration or enabled after bootup.
  – Next, disable OOD OPTIONS.
  – Switchover happens.

  Workaround: Reload the standby router once after the OOD OPTIONS configuration changes from enabled to disabled.

- CSCuc77283

  Symptoms: Upon reload or OIR, the CFM MEP configuration on an xconnect EFP is removed and cannot be reconfigured.

  Conditions: This symptom is observed with a CFM MEP on xconnect service instance. This issue is seen when reload or OIR is performed.

  Workaround: Remove the domain configuration.

- CSCuc77704

  Symptoms: The GETVPN/GDOI Secondary Cooperative Key Server (COOP-KS) does not download the policy (that is, when the **show crypto gdoi ks policy** command is issued on the Secondary COOP-KS and the command output shows that no policy is downloaded) and Group Members (GMs) registering to the Secondary COOP-KS fail to register without any warning/error message.

  Conditions: This symptom is observed when the GETVPN/GDOI group (with COOP configured) has an IPsec profile configured with one of the following transforms in its transform-set:

  – esp-sha256-hmac
  – esp-sha384-hmac
  – esp-sha512-hmac

  Workaround: Use esp-sha-hmac as the authentication transform instead.

- CSCuc77833

  Symptoms: “show int bri” returns no output.

  Conditions: This symptom is observed when router is loaded with the Cisco IOS Release 15.3(1.2)T image.

  Workaround: There is no workaround.

- CSCuc78772

  Symptoms: CPU watchdog is observed, followed by the box crashing.

Conditions: This symptom occurs when an IPv6 ACL entry is created with the log option. If there are more than 16 different traffic matching this ACL with a high rate, the box will run out of CPU to send to the log.

Workaround: Remove the log option from the ACL entry or create a more specific ACL to get less than 16 different traffic matching the same ACL entry.

- CSCuc79143

  Symptoms: The cellular driver should handle the profile getting inactive and should bring down the cellular interface.

  Conditions: This symptom occurs when the profile is deactivated by the HA.

  Workaround: Doing a “clear line” will bring down the cellular interface and restore the connection.

- CSCuc81117

  Symptoms: The router crashes with the **reload warm** command.

  Conditions: This symptom occurs when configuring “warm-reboot” with Cisco IOS Release 15.3(1.2)T.

  Workaround: Remove the **warm-reboot** command.

- CSCuc82224

  Symptoms: When a dynamic-EID host moves from one site to another, the hosts at the old site may not be able to communicate with the host that moved away.

  Conditions: This symptom occurs if the xTR at the old site had a map-cache entry for the dynamic-EID host that moved, for example, due to lig self. Then, this map-cache entry prevents communication after the dynamic-EID host moved away.

  Workaround: Clear the map-cache entry for the host prefix in question.

- CSCuc82551

  Symptoms: A Cisco ASR 1001 running Cisco IOS XE Release 3.6.2S or Cisco IOS XE Release 3.7.1S crashes with SNMP traffic.

  Conditions: This symptom is observed with SNMP polling with an IP SLA configuration.

  The crash signature is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SNMP ENGINE
  ```

  Workaround: Remove the SNMP configuration from the router or schedule the probe before polling via SNMP.

- CSCuc82992

  Symptoms: The router crashes upon execution of “no crypto engine slot 0” when the 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.

- CSCuc83104

  Symptoms: Path confirmation fails for blind transfer scenarios for both SIP Line and trunk-side scenarios.

  Conditions: This symptom is observed if “no supplementary-service sip refer” is configured.

  Workaround: Configure “supplementary-service sip refer”.

- CSCuc85321

  Symptoms: Cisco IOS may crash when AnyConnect is used.

  Conditions: This symptom is observed with the following conditions:

  - The router is configured as the SSL VPN gateway.
  - AnyConnect users make VPN connections to this router.

  Workaround: There is no workaround.

- CSCuc88175

  Symptoms: When a dynamic cryptomap is used on the Virtual Template interface, SAs do not created and thus the testscripts fail. This issue occurs because the crypto map configurations are not added to the NVGEN, and hence there is no security policy applied on the Virtual Template interface.

  Conditions: This symptom occurs only when a dynamic map is used on the Virtual Template interface. However, this issue is not seen when tunnel protection is used on the Virtual Template interface or when a dynamic map is used on the typical physical interface.

  Workaround: There is no workaround apart from using tunnel protection on the Virtual Template interface.

- CSCuc91717

  Symptoms: The router crashes when making basic x25 configuration change.

  Conditions: Remove x25 translation statement from running configuration when traffic is on.

  Workaround: Shut the interface before making x25 configuration change.

- CSCuc92167

  Symptoms: SSH use of Diffie-Hellman exchange to negotiate keying material is insecure and may lower the security of Diffie-Helman exchange.

  Conditions: This symptom occurs when there are known attacks against DH that takes effort of the effectively halving the length of the private key. Due to SSH use of DH private values of certain lengths, if the SSH is negotiated using AES-128 and HMAC-MD5, the time needed to recover the keys is lower than expected.

  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 3.6/3.2:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:S/C:P/I:P/A:N/E:POC/RL:U/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:
  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc93361

  Symptoms: "ip" protocol is not accepted in the **ping** command with the IPv6 address configured.

  Conditions: This symptom occurs when a single interface is configured with an IP address, and later, the mask alone is changed. For example:

  ```
  int e0/0
  ip addr 10.1.1.1 255.255.255.0
  no shut
  ```

  Later,

```
int e0/0
ip addr 10.1.1.1 255.255.0.0
```

Workaround: Configure a different IP address and then revert to the same address with the changed mask. For example:

```
int e0/0
ip addr 10.1.1.1 255.255.255.0
no shut
```

Later,

```
int e0/0
ip addr 10.1.1.2 255.255.0.0
ip addr 10.1.1.1 255.255.0.0
```

- CSCuc93739

  Symptoms: Phase 2 for the EzVPN client with split network and VTI does not come up if IPsec SA goes down.

  Conditions: This symptom occurs because IPsec SA is not being triggered after IPsec SA is down due to no traffic. So, in spite of traffic, IPsec SA is not coming up, leading to packet drops in the client network. The same problem is not seen with Cisco IOS Release 15.0(1)M7. This behavior is introduced post-PAL, where virtual-interface creates a ruleset where traffic cannot trigger IPsec SA again once IPsec SA is deleted.

  Workaround 1: Configure “ip sla” on EZVPN client for split networks, so IPsec SA will not go down.

  Workaround 2: Remove “virtual-interface” from the EZVPN client profile if that is not needed.

  Further Problem Description: The problem is not seen in Cisco IOS Release 15.2(4)M1 without virtual-interface.

- CSCuc94687

  Symptoms: SHA2 processing in software causes low throughput or high CPU.

  Conditions: This symptom is observed with the Cisco 892 with SHA2 configured and the onboard crypto engine enabled running Cisco IOS Release 15.2(4)M and later releases.

  Workaround: There is no workaround.

- CSCuc95160

  Symptoms: After receiving the CRCX message, the Cisco AS5400 does not send 200 ok to SSW. SSW sends the CRCX message to the Cisco AS5400 again. Between these messages, debug outputs are displayed. It seems that the call is not disconnected completely for the end point by the previous disconnect request (the DLCX is received after the CRCX message from SSW). The end point may be stuck in call_disconnecting state.

  Conditions: This symptom is observed with MGCP. This issue occurs when the Cisco AS5400 receives DLCX before sending 200 ok for the first CRCX message.

  Workaround: There is no workaround.

- CSCuc96241

  Symptoms: The Cisco Y.1731 Performance Monitoring SLM interworking between the Cisco ME3400 and the Cisco IOS-XR ASR 9000 is not functioning.

  Conditions: This symptom is observed when SLM is running on the Cisco ME3400 and Cisco IOS-XR ASR 9000 router.

  Workaround: There is no workaround.

- CSCuc96631

  Symptoms: Incoming calls through e1 r2 stop working in Cisco IOS Release 15.2(4)M1.

  Conditions: This symptom is observed with incoming calls through e1 r2 in Cisco IOS Release 15.2(4)M1. Outgoing calls work fine.

  Workaround: Use Cisco IOS Release 15.2(2)T.

- CSCuc98021

  Symptoms: One-way voice audio issue is seen over CUBE after session re-INVITE 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.

- CSCud01774

  Symptoms: Under an extremely rare occurrence, a router can crash during “no router ospf <pid>” execution.

  Conditions: This symptom is observed when there is a redistribute statement configured under the OSPF process.

  Workaround: There is no workaround.

- CSCud02357

  Symptoms: The extension mobility feature is failing.

  Conditions: This symptom is observed in Cisco IOS Release 15.3(2)T.

  Workaround: There is no workaround.

- CSCud02361

  Symptoms: Sequence number of spoofed ACK sent to the server has a 0x00 value.

  Conditions: This symptom occurs 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.

- CSCud02391

  Symptoms: The EIGRP routes are not coming up after removing and reenabling the tunnel interface.

  Conditions: This symptom is observed when EIGRP routes do not populate properly.

  Workaround: There is no workaround.

- CSCud03016

  Symptoms: The TCP HA connection gets closed with SSO disabled from standby.

  Conditions: This symptom is observed when the connection is initiated from a non-HA box to an HA box.

  Workaround: There is no workaround.

- CSCud03250

  Symptoms: The performance degradation was seen starting the XE37 throttle build 09/18 (BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025).

  Conditions: This symptom is observed when the user tries with BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label and the performance number is still good, but the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025 label image shows much higher performance numbers in the order of 400 seconds. This issue is seen when the user also tries with BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label with the CSCtz68303 fix patched in.

  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”.

- CSCud03646

  Symptoms: After SSO, sometimes the repair path over the remote LFA tunnel may point to drop adjacency.

  Conditions: This symptom is a race condition that appears infrequently in older code base.

  Workaround: Shut/no shut the interface to force the recreating the tunnel.

- CSCud05636

  Symptoms: The MAC-address gets corrupted when user sends the multicast traffic.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M3 image, where as the same multicast traffic works as expected with Cisco IOS Release 12.4T image.

  Workaround: A possible work around is to enable the **ip pim nbma- mode** command at the CPE end.

- CSCud06180

  Symptoms: When the SDK crash occurs, the cellular interface is not operational.

  Conditions: This symptom occurs when the IPSLA is present on the cellular interface, and you power-cycle the modem 8-10 times, causing the CWAN_SHIM layer to crash.

  Workaround: There is no workaround.

- CSCud06237

  Symptoms: Local ID is 0.0.0.0 in PfR target discover feature.

  Conditions: This symptom is seen when manual EIGRP is used for PfR target discover feature.

  Workaround: There is no workaround.

  Further Problem Description: A site will not be able to publish its local prefixes.

- 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.

- CSCud07504

  Symptoms: SRE-WAAS optimized traffic gets dropped by ZBFW.

  Conditions: This symptom occurs when ZBFW, WCCP, and SRE-WAAS are configured.

  Workaround: There is no workaround.

- CSCud08166

  Symptoms: The Cisco ASR 1000 router crashes with “Exception to IOS Thread” and the following error:

  ```
  "UNIX-EXT-SIGNAL:
  Segmentation fault(11), Process = Virtual Exec"
  ```

  Conditions: This symptom is observed when an ACL used with “ip pim rp-address” is moved from standard to extended and “no ip multicast-routing” is configured (either in global or in a mVRF). The standard ACL must be deleted and recreated as extended, for example:

  The following series of commands are necessary to trigger the crash:

  ```
  <begin-config>
  !
  ip multicast-routing
  !
  ip pim rp-address 10.200.255.42 STATIC-RP-LN-SERVER-FARMS override
  !
  no ip access-list standard STATIC-RP-LN-SERVER-FARMS
  ip access-list extended STATIC-RP-LN-SERVER-FARMS
   remark -- STATIC RP LN SERVER FARMS MCAST GROUP ACL --
   permit ip 239.255.0.0 0.0.255.255 any
   permit ip 224.0.0.0 15.255.255.255 any
  !
  !
  no ip multicast-routing
  <end-config>
  ```

  Workaround: Crash can be prevented by any of the following methods:

  1. Disassociate the standard ACL from “ip pim rp-address” before deleting ACL. For example:

     ```
     no ip pim rp-address 10.200.255.42 STATIC-RP-LN-SERVER-FARMS override
     ```

     and then

     ```
     no ip access-list standard STATIC-RP-LN-SERVER-FARMS
     ```

2. Do not convert a standard ACL to extended while it is still being referenced in “ip pim rp-address”. Use a new name for the new extended ACL.
3. Do not disable multicast routing using “no ip multicast-routing”.

- CSCud08595

  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to multiframe established.

  Conditions: This symptom occurs 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.

- CSCud09870

  Symptoms: The device crashes when you enable “debug cmd-cfm” over xconnect with PC.

  Conditions: This symptom is observed when you configure the cfm over xconnect with PC downmep. After enabling the **debug** command, the device crashes.

  ```
  debug ethernet cfm pm session db 0
  ```

  Workaround: Issue the **undebug** command.

- CSCud13862

  Symptoms: The Cisco WS-SUP720 running Cisco IOS Release 12.2(33)SRE3 crashes.

  Conditions: This symptom occurs during a CPU process history update.

  Workaround: The issue can be avoided by removing the configuration statement for “CPU Utilization Statistics”.

  ```
  conf t
    no process cpu statistics limit
  ```

- CSCud21066

  Symptoms: The Cisco IOS Scansafe feature is not supported on c880voice-universlk9-mz images.

  Conditions: This symptom is observed when using the Cisco 880 series routers, when the voice image cannot turn on scansafe.

  Workaround: There is no known workaround.

- 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: This symptom occurs if metric-style wide is configured for only one level on the router running both levels, and fast-reroute is configured.

  Workaround: Configure metric-style wide for both levels (by default).

- CSCud25043

  Symptoms: A WebVPN-enabled gateway crashes on Cisco IOS Release 15.1(4)M5 due to SSLVPN_PROCESS.

  Conditions: This symptom is observed under the following conditions:

  – Cisco IOS Release 15.1(4)M5
  – SSL VPN (WebVPN enabled)

  Workaround: There is no workaround.

- CSCud26189

  Symptoms: The map cache entries are lost after RP switchover when lisp_patr is configured.

  Conditions: This symptom occurs after RP switchover.

  Workaround: There is no workaround.

- CSCud27379

  Symptoms: WS-SUP720-3B running Cisco IOS Release 12.2(33)SRE4 crashes at get_alt_mod after issuing “sh run int g4/13” with several trailing white spaces until the cursor stops moving.

  Conditions: This symptom occurs when you issue the **show run interface** command with trailing spaces until the cursor stops moving.

  Workaround: Do not specify trailing spaces at the end of the **show run interface** command.

- CSCud31808

  Symptoms: With the two commands configured listed under the conditions of this release note, the Cisco router might start advertising a low TCP receive window size to the TCP peer for a specific TCP transaction. The value of this receive window size becomes equal to the configured MSS value, and it will never exceed this value anymore. This might impact TCP performance.

  Conditions: This symptom happens only if the following two commands are configured on the router:

  – **ip tcp mss x**

  – **ip tcp path-mtu-discovery**

  Workaround: Either change the path-mtu discovery ager timeout to 0, or remove one of the two commands.

- 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.

- CSCud34809

  Symptoms: ISM will not encrypt on a single tunnel. It may continue to decrypt. Over a period of time, the number of such tunnels might increase.

  Conditions: This symptom is observed after rekey occurs several times, and a single tunnel may not encrypt.

  Workaround: There is no workaround.

- CSCud36113

  Symptoms: Ping fails between CE routers.

  Conditions: This symptom is observed when you configure MPLS VPN Inter-AS IPv4 BGP Label Distribution and flaps “mpls bgp forwarding” in the interface between ASBRs.

  Workaround: Removing and adding (flapping) the static routes between ASBRs resolves the issue.

- CSCud36208

  Symptoms: The multilink ID range has to be increased from the existing 65535.

  Conditions: This symptom is observed specifically with the Cisco MWR1.

Workaround: There is no workaround. The range is now made configurable based on PD.

- CSCud36723

  Symptoms: RPF information for IPv6 multicast mroutes is not updated when routing changes.

  Conditions: This symptom occurs when an IPv6 multicast configuration is present in the startup-configuration.

  Workaround: After startup, remove all IPv6 multicast configurations, if any, and then apply the configuration as needed.

- CSCud38774

  Symptoms: The router is showing CPU utilization at 99%. LDAP seems to be hogging the CPU process.

  Conditions: This symptom can occur randomly at any point of time where NTLM authentication is deployed. This issue is observed only when the server is not able to handle the churn of requests and requests are being stuck at Bind On-Going state, which can be verified with **show ldap server** *server-name* **connections**.

  Workaround: Clearing LDAP server connections helps in resolving this issue:

  **clear ldap server** *server-name*.

- CSCud42529

  Symptoms: The router crashes when receiving IPv6 ICMP packet.

  Conditions: This symptom is observed when ISM-VPN is used as a crypto engine. This issue does not occur when using an onboard crypto engine.

  Workaround: There is no workaround.

- CSCud42938

  Symptoms: After a **clear crypto session**, sometimes ident SM remains at responder side.

  Conditions: This symptom occurs when doing a **clear crypto session** multiple times, the crypto map is deleted, but ident remains due to a race condition between new connections also coming up. Since the map is removed and ident remains, the new connections never come up.

  Workaround: Reboot the router.

- CSCud43620

  Symptoms: The Gateway fails to send ACK after 200 OK while testing DNS/SRV Lookup on a VOIP peer with weight/priority.

  Conditions: This symptom is observed when a Cisco router is loaded with the c2900-universalk9-mz.SSA.153-1.7.T image.

  Workaround: There is no workaround.

- CSCud46314

  Symptoms: The Cisco router crashes when polling ciscoEnvMonSupplyStatusDescr MIB.

  Conditions: The ciscoEnvMonSupplyStatusDescr MIB is getting polled.

  Workaround: Apply the following to block the view:

  - snmp-server view blockmib iso include
  - snmp-server view blockmib 1.3.6.1.4.1.9.9.13.1.5.1.2 exclude

  Similarly, apply the following to the community:

  - snmp-server community <community> view blockmib ro

- CSCud51791

  Symptoms: Memory leak is seen on the router related to CCSIP_SPI_CONTRO.

  Conditions: This symptom is observed in CME SIP phones with Presence in the running-configuration.

  Workaround: There is no workaround. You may try to remove Presence from the running-configuration.

- CSCud53687

  Symptoms: Packets sourced from a registered application port for which ALG support is present may be incorrectly classified as ALG, and therefore the session is dropped.

  An example is an application that uses TCP source port 1720 to establish a connection with a remote device. The router performing NAT incorrectly marks this packet as needing ALG processing ultimately resulting in the connection failing.

  Conditions: This symptom occurs when you use one of the registered source ports that support ALG processing and NAT.

  Workaround: You can disable the NAT ALG fixup for the particular protocol which port number matches with the non-ALG traffic's source port. But this will restrict the coexistence of ALG as well as non-ALG traffic with the same source port.

- CSCud53872

  Symptoms: After a reload on the Cisco ASR 1000 series router, several key syslogs are sent with the incorrect source address for a few seconds. Due to the wrong source address, the syslogs are dropped at the collector end.

  Conditions: This symptom is observed when the loopback interface is configured as the source address of the syslogs.

  Workaround: There is no workaround.

- CSCud54365

  Symptoms: The scansafe socket is not closed by reset from the client

  Conditions: This symptom occurs when sending a connection request from the client (SYN packet). This issue is seen when ack is sent instead of syn+ack for a syn request from the server. The client will send a Reset(RST) signal for ack received instead of syn+ack. The L4F/scansafe box displays that the flow is not closed.

  Workaround: Make sure that the server does not have a stale TCP tuple flow entry before trying for a connection from the client.

- CSCud56400

  Symptoms: Build breakage occurs due to CSCub81489 partial export to mcp_dec.

  Conditions: This symptom is observed with export to mcp_dec.

  Workaround: There is no workaround.

- CSCud57414

  Symptoms: The system crashes when monitoring traffic with performance monitoring policies on the incoming and outgoing interfaces.

  Conditions: This symptom is observed when a large number of flows is being monitored and traffic changes.

  Workaround: Redefine the match criteria to reduce the number of flows generated with the type of traffic being monitored.

- CSCud58633

  Symptoms: The “initial-contact” configuration option not needed, as the behavior is already enabled.

  Conditions: This symptom is observed when you use IKEv2, along with Cisco IOS Release 15.2(4)M.

  Workaround: There is no workaround.

- CSCud61276

  Symptoms: The Cisco ASR 901 may crash while running an automated test script containing several tests to test the multi-nni feature.

  Conditions: This symptom occurs when you run the automated tests several times.

  Workaround: Do not run the test script (configure manually).

- CSCud61517

  Symptoms: CUBE crashes during a blind-transfer scenario and when “media preference IPv6” is configured.

  Conditions: This symptom occurs only when “media preference IPv6” is configured but is not seen when “media preference IPv4” is configured.

  Workaround: Configure “media preference IPv4”.

- CSCud62774

  Symptoms: The values reported for “application media packets rate variation [sum]” may be incorrect. The functionality of Media Rate Variation TCA (Threshold Crossing Alarm) may also be impacted by this.

  Conditions: This symptom is observed when the user wants to obtain MRV metrics by including the following command in the Performance Monitor flow record configuration:

  ```
  application media packets rate variation [sum]
  ```

  Workaround: There is no workaround.

- CSCud64506

  Symptoms: HQF does not clear up when the Bandwidth remaining ratio is misconfigured on the Child Policy.

  Conditions: This symptom is observed when an incorrect configuration triggers the policy rejection and fails on the cleanup with the nondefault queue-limit setting in the class-default class.

  Workaround: Apply the configuration with the correct setting.

- CSCud65119

  Symptoms: A crash may occur while using GETVPN with fragmented IPv6 traffic.

  Conditions: This symptom occurs when IPv6 IPsec is used. This issue is triggered by fragmented IPv6 packets.

  Workaround: There is no workaround.

- CSCud65150

  Symptoms: The device might crash randomly due to an address error, as follows:

  ```
  16:14:04 CST Fri Nov 30 2012: Address Error (load or instruction fetch)
exception, CPU signal 10, PC = 0x22895480
  ```

  Conditions: This symptom was first seen on a Cisco 2911 router. The crash is triggered randomly some time after a Kron Policy runs a TCL script:

```
kron occurrence ipchange in 5 recurring system-startup
  policy-list tcl_script

kron policy-list ipchange
  cli tclsh flash:/SCRIPT.tcl
```

Workaround: Remove the Kron configurations from the system.

- CSCud66669

  Symptoms: On the Cisco 7200, the tunnel is established correctly and encryption and decryption occur correctly. However, after decryption, the packet is not punted to the iVRF in which the tunnel interface resides, leading to a broken IPSec-DataPath.

  Conditions: This symptom is observed with the Cisco 7200 with VSA under the following conditions:

  - Tunnel (GRE/mGRE) in an iVRF with Tunnel protection configuration.
  - iVRF not equal to fVRF.

  Workaround: This issue has been observed with Cisco IOS Release 15.0(1)M9 and Cisco IOS Release 12.4(24)T8, so downgrade might be an option. There is no known configuration-related workaround yet, although software crypto will work just fine.

- 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 xfer, along with the “headset auto-answer” configuration in the ephone.

  Workaround: Remove the “headset auto-answer” configuration in the ephone configuration.

- CSCud67792

  Symptoms: An invalid modem is detected.

  Conditions: This symptom is observed during bootup.

  Workaround: Use Cisco IOS Release 15.2T-based images.

- CSCud68178

  Symptoms: The Cisco ASR 1000 series router and Cisco ISR 4400 series hubs crash.

  Conditions: This symptom occurs when the physical and tunnel interface are flapping.

  Workaround: There is no workaround.

- CSCud69078

  Symptoms: In a GETVPN setup, when using the ISM module, decryption fails and the original (ESP) packet gets forwarded to a destination which eventually will get dropped.

  Conditions: This symptom is observed when the same GETVPN crypto map is applied on two or more different interfaces on the router with ISM.

  Workaround:

  1. Switch to onboard or sw encryption.
  2. To get encryption/decryption working on one interface, remove the crypto map from both interfaces, shut/no shut both interfaces, and then reapply the crypto map on one of the interfaces.

- CSCud69592

  Symptoms: The Call Progress Analysis (CPA) feature does not work. Though DSP is allocated and programmed for the CPA functionality, no CPA events are detected and reported.

  Conditions: This symptom is observed for those call flows, where media bridging occurs after 200 OK responses.

  Workaround: There is no workaround.

- CSCud70629

  Symptoms: Incremental memory leaks are seen at IPSec background proc.

  Conditions: This symptom is observed with “clear nhrp cache”.

  Workaround: There is no workaround.

- CSCud71773

  Symptoms: The **cost-minimization** test command is not accepted.

  Conditions: This symptom is observed with the **cost-minimization** test command.

  Workaround: There is no workaround.

- CSCud74552

  Symptoms: Ping on the EHWIC-1GE-SFP-CU interface fails.

  Conditions: This symptom is observed when ISM-VPN is installed. However, it is not necessarily utilized for encryption/decryption.

  Workaround: There is no workaround.

- CSCud78618

  Symptoms: Router crashes.

  Conditions: This symptom is seen when applying IVRF configuration on IKE profile.

  Workaround: There is no workaround.

- CSCud83835

  Symptoms: An IPsec VPN tunnel fails to be established. The **debug crypto ipsec** command shows no output when attempting to bring up the tunnel.

  Conditions: This symptom occurs when all of the following conditions are met:

  1. The crypto map is configured on a Virtual-Template interface.
  2. This Virtual-Template interface is configured with “ip address negotiated”.
  3. The tunnel is initiated locally (in other words, if the tunnel is initiated by the peer, it comes up correctly).

  Workaround: Downgrade to Cisco IOS Release 15.2(2)T3 or earlier releases or always initiate the VPN tunnel from the peer.

- CSCud86082

  Symptoms: Abnormal CPUHUG is observed when doing “config replace”.

  Conditions: This symptom is observed with “config replace” in a LISP scaling configuration.

  Workaround: There is no workaround.

- CSCud86954

  Symptoms: Some flows are not added to the Flexible Netflow cache, as indicated by the "Flows not added" counter increasing in the **show flow monitor statistics** command output. "Debug flow monitor packets" shows "FNF_BUILD: Lost cache entry" messages, and after some time, all cache entries are lost. At that moment, debug starts showing "FLOW MON: ip input feature builder failed on interface couldn't get free cache entry", and no new entries are created and exported ("Current entries" counter remains at 0).

  The following is sample output when all cache entries are lost:

```
Router#sh flow monitor FNF-MON stat
  Cache type:                                 Normal
  Cache size:                                   4096
  Current entries:                                 0
  High Watermark:                                882

  Flows added:                                 15969
  Flows not added:                             32668
  Flows aged:                                  15969
    - Active timeout      (  1800 secs)            0
    - Inactive timeout    (    15 secs)        15969
    - Event aged                                   0
    - Watermark aged                               0
    - Emergency aged                               0
```

  Conditions: This symptom occurs when all of the following are true:

  – Flexible Netflow is enabled on a DMVPN tunnel interface.

  – Local policy-based routing is also enabled on the router.

  – Local PBR references an ACL that does not exist or an ACL that matches IPsec packets.

  Workaround: Make sure that the ACL used in the local PBR route-map exists and does not match IPsec packets sent over the DMVPN tunnel interface.

- CSCud89684

  Symptoms: The snmp-server community public string is not nvgened .

  Conditions: This symptom occurs when the snmp-server host is configured with the same community name after configuring **snmp-server community** command.

  Workaround: There is no workaround.

- CSCud90568

  Symptoms: The Input queue of an interface shows 76/75. In "show buffers input-interface interface packet", you will find UDP packets with the port used by DTLS.

  Conditions: This symptom is observed with SSLVPN with DTLS enabled (it could be enabled by default, depending on the platform).

  Workaround: Disable DTLS. Reload.

- CSCud95387

  Symptoms: Call transfer with Trombone and ANAT fails.

  Conditions: This symptom occurs when CUBE is configured with ANAT and Antitrombone, and during call transfer, the call fails due to wrong media negotiation.

  Workaround: Disable ANAT.

- CSCud95940

  Symptoms: A Cisco 3900 running with CME and Skinny Phones could experience CPUHOGs and a Watchdog, resulting in a crash.

```
%SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
(630/222),process = Skinny Msg Server.
-Traceback= 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Skinny Msg Server.
-Traceback= 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX
```

  Conditions: This symptom is observed with Cisco 3900 running with CME and Skinny Phones.

  Workaround: There is no known workaround.

- CSCud96075

  Symptoms: A router running Cisco IOS Release 15.2(4)M2 will reload with a bus error soon after the DSP reloads when there is a live transcoding session.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)M2.

  Workaround: There is no workaround.

- CSCud98366

  Symptoms: In a multi-home MLDP inband setup with different RDs configured, there is no MLDP state on ingress PE if BGP best path is different than multicast RPF PE.

  Conditions:

  1. MLDP inband profile is configured in multi-home setup with different RDs.
  2. BGP chosen best path is different than chosen RPF PE for multicast.

  Workaround: Configure route policy on egress PE such that chosen RPF PE is same as BGP best path.

- CSCud99034

  Symptoms: Data encapsulation fails in the Cisco IOS Release 15.3(1.11)T image.

  Conditions: This symptom occurs when ISM-VPN is enabled as the crypto engine.

  Workaround: Disable ISM-VPN and use either the Onboard crypto engine or the Software crypto engine.

- CSCue04709

  Symptoms: The following error message is displayed:

```
sh mpls l2t vc detail show VC down with AC rx/tx faults
Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: DOWN AC(rx/tx faults)
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: DOWN AC(rx/tx faults)
```

  Conditions: This symptom is an intermittent issue seen on a new standby RP after an RP switchover when a second fault, that is, the dataplane fault occurs while the VC is still recovering from RP failover.

  Workaround: Remove the “aaa new-model” configuration and reconfigure xconnect.

- 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.

- CSCue35533

  Symptoms: Ping fails with security applied and IKE disabled.

  Conditions: This symptom is observed when the Cisco IOS Release 15.3(1.15)T image is loaded.

  Workaround: There is no workaround.

- CSCue36321

  Symptoms: A crash occurs when MLP is configured.

  Conditions: This symptom is observed with an MLP configuration.

  Workaround: There is no workaround.

- CSCue39206

  Symptoms: ES crashes after the second 401 challenge.

  Conditions: This symptom occurs when the second 401 is received after SDP offer/answer with 183/PRACK is complete. This is a rare scenario.

  Workaround: There is no workaround.

- CSCue46198

  Symptoms: The router crashes when RITE is applied.

  Conditions: This symptom occurs when RITE is applied on the interface.

  Workaround: Remove the RITE from the interface.

- CSCue46590

  Symptoms: HTTP POST messages may not be fixed properly after adding scansafe headers.

  Conditions: This symptom was first identified on a Cisco ISR running a Cisco IOS Release 15.2(4)M2 image. A Cisco IOS Release 15.2(4)M1 image does not show the problem.

  Workaround: Whitelist the domain from being sent over to the towers.

- CSCue51886

  Symptoms: The SBC CUBE device rejects call connections.

  Conditions: This symptom is observed when the Chunkmanager holds a lot of memory and calls do not get processed.

  Workaround: Reloading the box helps to make the box stable.

- CSCue59775

  Symptoms: The device crashes.

  Conditions: This symptom is observed when the service-policy is removed.

  Workaround: There is no workaround.

- CSCue77265

  Symptoms: Increment memory leaks are seen at IPSec background proc.

  Conditions: This symptom occurs when “clear cry session” is issued multiple times when bringing up the tunnel.

  Workaround: There is no workaround.

# Caveats for Cisco IOS Release 15.3(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.

**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. (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 15.3(1)T1

All the caveats listed in this section are resolved in Cisco IOS Release 15.3(1)T1. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCta80024

  Symptoms: The router crashes while using the **string repeat** command with the biggest number in the TCL shell.


**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

Conditions: This symptom occurs when the **string repeat** command is used with the biggest number. This issue also depends on the string being used. For example, the below commands in the TCL shell will lead to crashing of the router.

```
proc demo foo "set bar [string repeat {$foo} 255]"
demo [string repeat a 16843010]; concat
```

Workaround: There is no workaround.

- CSCtg82170

  Symptoms: The IP SLA destination IP/port configuration changes over a random period of time. This issue is hard to reproduce but has been reported after upgrading to Cisco IOS Release 15.1(1). So far, it only seems to have affected the destination IP and port. The destination IP may be changed to an existing destination IP that has already been used by another probe. The destination port is sometimes changed to 1967 which is reserved for IP SLA control packets. Other random destination ports have also been observed to replace the configured port for some of the IP SLA probes. Each time when the change happens, many of the IP SLA probes will stop running.

  Conditions: This symptom is observed in Cisco IOS Release 15.1(1)XB and Cisco IOS Release 15.1(1)T. Other Cisco IOS versions may also be affected.

  Workaround: A possible workaround is to downgrade to any Cisco IOS versions older than Cisco IOS Release 15.1.x.

- CSCtr87413

  Symptoms: Static route that is injected by "reverse-route static" in crypto map disappears when the router receives the delete notify from the remote peer. Static route also gets deleted when DPD failure occurs.

  Conditions: The symptom is observed when you configure "reverse-route static" and then receive a delete notify or DPD failure.

  Workaround: Use **clear crypto sa**.

- CSCts75737

  Symptoms: Tracebacks are seen at swidb_if_index_link_identity on the standby RP.

  Conditions: This symptom is observed when unconfiguring and reconfiguring "ipv4 proxy-etr" under the router LISP.

  Workaround: There is no workaround.

- CSCtw65575

  Symptoms: The router may unexpectedly reload when OSPFv3 MIB is polled via SNMP.

  Conditions: This symptom occurs when OSPFv3 is configured with area ranges whose prefix length is /128. A router with no area ranges is not vulnerable.

  Workaround: Configure area ranges to have a smaller prefix length (that is, in the range of /0 to /127).

- 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. 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”.

- 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.

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCty44654

  Symptoms: The router crashes when trying to test the MVPN6 functionality.

  Conditions: This symptom is observed with the following conditions:

  – Configure the router to test the MVPN6 functionality.

  – Delete the VRF associated with the interface in the MVPN6 test configuration.

  Workaround: There is no workaround.

- CSCty57476

  Symptoms: The BGP GSHUT feature needs to add support for the AA:NN format for community.

  Conditions: This symptom is observed when support is added for the AA:NN format for community when using the BGP GSHUT feature.

  Workaround: The <1-4294967295> community number can be used instead of the AA:NN format.

- 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.

- 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:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCua47056

  Symptoms: The Cisco Catalyst 6000 crashes after the removal of the supervisor module from active VSS with the following traceback:

  ```
  0x41048F64 ---> ospf_rcv_dbd+F48 0x41041FE8 ---> ospf_router+548 0x4166C0B0 --->
  r4k_process_dispatch+14 0x4166C09C ---> r4k_process_dispatch
  ```

  Conditions: This symptom occurs when the following reproduction procedure is performed:

  NSF is disabled including helper using the below given commands:

  ```
  router ospf <AS>
  no nsf
  nsf cisco helper disable
  ```

  Adjacency flapped.

  NSF enabled again.

  Performed switchover.

  Workaround: Avoid the reproduction procedure in the production. Neighbors should see the router configured for "nsf cisco" as OOB resync capable:

  ```
  Router#sh ip ospf nei <interface> detail
  ...
      LLS Options is 0x1 (LR)   <-- LR bit means OOB resync capability
  ...
  ```

  If the router is configured for the "nsf cisco", but the neighbor does not see LR bit set for router with "nsf cisco", flap the adjacency, and OOB resync capability will be renegotiated.

- 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.

- 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.

- CSCua76157

  Symptoms: BGP routes are displayed.

  Conditions: This symptom occurs after removing the “send-label” from PE.

  Workaround: There is no workaround.

- CSCua78782

  Symptoms: Authentication of EzVPN fails.

  Conditions: The symptom is observed with BR-->ISP-->HQ.

  Workaround: There is no workaround.

- CSCub04982

  Symptoms: In an IPFRR configuration, a traceback is seen about changing the FRR primary OCE where the new OCE has a different interface and next-hop, which blocks such a linkage.

  Conditions: This symptom occurs while changing the FRR primary OCE interface to a new OCE with a different interface.

  Workaround: There is no workaround.

- CSCub14145

  Symptoms: A Cisco ISR-G2 with VPN-ISM logs output similar to:

  ```
  !! Cannot find ISM-VPN counters struct for flowid: 0x44000084
  ```

  Conditions: This symptom is observed when using a VPN-ISM in an IPsec deployment with images from the Cisco IOS 15.2 train.

Workaround: There is no workaround.

Further Problem Description: The issue is cosmetic in nature while the VPN-ISM is queried for counters, for example, **show** commands.

- CSCub38559

  Symptoms: When static recursive routes are used in an MVPNv6 environment, multicast traffic loss can occur due to failure to determine the correct RPF interface for a multicast source or rendezvous point.

  Conditions: This symptom occurs if a static route to an IPv6 address at a remote site (remote side of a VPN cloud) resolves via a BGP route, resulting in a failure to install the required MDT alternate next-hop in the recursively referenced BGP route.

  Workaround: Executing “show ipv6 rpf vrf X <address>” for any address within the recursively referenced BGP prefix range will cause installation of the required alternate next-hop.

- CSCub44898

  Symptoms: Stale scansafe sessions are seen on the router. They do not get cleared even with the **clear content-scan sessions *** command.

  Conditions: This symptom occurs when one of the end points (client or server) does not properly close the connection. In TCP terms, when one end does not send an ACK to the FIN request sent by the other end in L4F UNPROXIED state.

  Workaround: There is no workaround. The router needs to be rebooted to clear the stale sessions.

- 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

- CSCub56064

  Symptoms: Ping fails after doing EZVPN client connect if CEF is enabled.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(0.8)T image. This issue is seen only for a specific topology, where the in/out interface is the same.

  Workaround: There is no workaround.

- CSCub74272

  Symptoms: Intermittently during Phase II rekey, after new SPIs are negotiated and inserted into SPD, old SPIs are removed and then the VTI tunnel line protocol goes down.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T, with VTI over GRE.

  Workaround: There is no workaround.

- CSCub76103

  Symptoms: When callback tries to send a message, there is a traceback.

  Conditions: This symptom is observed when you set the call-home profile’s transport to HTTP 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
```

- CSCub80386

  Symptoms: The following interface configuration should be used:

  ```
  interface Ethernet2/1
  description lanethernet1
  ipv6 enable
  ospfv3 100 network manet
  ospfv3 100 ipv6 area 0
  ```

  Dead interval is calculated according to network type; in this case, it is 120s. Issue the **no ospfv3 dead-interval** command on dead interval. Dead interval is set to the default of 40s instead of 120s, which is correct for manet or P2MP interface types.

  Conditions: This symptom is an OSPFv3-specific issue (see the configuration example).

  Workaround: Configure dead interval explicitly or reapply the network command.

- CSCub80710

  Symptoms: SSL handshake between Cisco VCS and the Cisco ASR fails if the Cisco ASR is running Cisco IOS XE Release 3.7S.

  Conditions: This symptom occurs in a working setup, if the Cisco ASR is upgraded to Cisco IOS XE Release 3.7S, then SSL handshake and subsequently SIP-TLS calls start to fail. If in the same setup, the Cisco ASR is downgraded back to Cisco IOS XE Release 3.5S or Cisco IOS XE Release 3.4.4S, then the calls work (without requiring any additional changes).

  Workaround: There is no workaround.

- CSCub85451

  Symptoms: When "Scan Safe" is enabled on the interface, latency may be seen. Some pages may not load at all or show severe latency if the SYN request sent by the ISR does not receive an appropriate SYN ACK response from the Scan Safe Tower.

  Conditions: This symptom occurs when "Scan Safe" is enabled on the interface. In this case, there was an ASA in the path that enabled sequence number randomization.

  Workaround: Disable sequence number randomization on the firewall in the path before the ISR.

  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-2012-4651 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

- CSCub89144

  Symptoms: In a VTI scenario with HSRP stateless HA, the tunnel state on standby is up/up.

  Conditions: This symptom occurs when HSRP is configured and there is no SSO configuration.

  Workaround: There is no workaround.

- CSCub95261

  Symptoms: The device crashes due to a bad reference count:

```
%SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count, chunk 40A82BB4
data 313E2F40 refcount FFFFFFFF alloc pc
2341E7F4. -Process= "CSDB Timer process", ipl= 3, pid= 274
-Traceback= <HEX TRACEBACK HERE>

chunk_diagnose, code = 3
chunk name is CSDB l4 structu

current chunk header = 0x313E2F30
data check, ptr = 0x313E2F40

next chunk header = 0x313E2F90
data check, ptr = 0x313E2FA0

previous chunk header = 0x313E2ED0
data check, ptr = 0x313E2EE0
```

Conditions: This symptom occurs only when IPS is enabled on the router. The likelihood of the defect increases when there is a sudden surge of concurrent short-lived flows, for example, SYN floods.

Workaround: Disable IPS.

- 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.

  Workaround: There is no workaround.

- CSCuc08061

  Symptoms: IPv6 DMVPN spoke fails to rebuild tunnels with hubs.

  Conditions: This symptom occurs when the tunnel interface on the spoke is removed and reapplied again.

  Workaround: Reboot the spoke.

- CSCuc09483

  Symptoms: Under certain conditions, running a TCL script on the box may cause software traceback and reload of the affected device.

  Conditions: This symptom occurs when a Privilege 15 user may run TCL commands that may lead to an affected device reloading.

  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 3.8/3.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:S/C:N/I:N/A:C/E:F/RL:U/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:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc14088

  Symptoms: The default class is not being exported with the class option template.

  Conditions: This symptom occurs when class-default is not exported when typing the option c3pl-class-table under the flow exporter.

  Workaround: There is no workaround.

- CSCuc15695

  Symptoms: The counters are not polling the correct stats.

  Conditions: This symptom was first observed on the ATM interfere, but it is not particular to the ATM as this issue was reproduced on the Gigabit Ethernet interface as well.

  Workaround: There is no workaround.

- 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.

  Workaround: There is no workaround.

  Further Problem Description: So far, this issue is only seen in the FFM performance test script.

- CSCuc19862

  Symptoms: Traceback and CPU hog is seen due to spurious memory access when Flexible NetFlow (FNF) is enabled.

  Conditions: This symptom is seen when enabling FNF.

  Workaround: Use classic netflow or configure FNF on the tunnel template interface (preferred).

  Note: the first option of using classic netflow is not available on some platforms which only support FNF. Notably these are Cat 6k, Sup 2T and the Cat 4K K10.

- CSCuc31725

  Symptoms: CUBE fails to resolve the configured DNS through A query when the SRV query fails.

  Conditions: This symptom occurs when running Cisco IOS Release 15.3(0.11)T.

  Workaround: Use DNS SRV records for SIP servers.

- CSCuc37047

  Symptoms: VSS crashes on reconfiguring “ipv6 unicast-forwarding” multiple times.

  Conditions: This symptom occurs when CTS is configured on an interface and “ipv6 unicast” is toggled multiple times.

  Workaround: There is no workaround.

- CSCuc44438

  Symptoms: There is a memory corruption issue with loading NBAR protocol pack.

  Conditions: This symptom occurs when an NBAR protocol pack is loaded into the router using the **ip nbar protocol-pack** command.

  Workaround: There is no workaround.

- CSCuc45115

  Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.

Conditions: This symptom is observed in the case where there are two Overlay addresses of a different Address Family on the same NBMA (such as IPv4 and IPv6 over IPv4). This issue is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

Workaround: There is no known workaround.

- CSCuc45528

  Symptoms: Leaks are seen at nhrp_recv_error_indication.

  Conditions: This symptom occurs only when the fix of CSCub93048 is present in the image.

  Workaround: There is no workaround.

- CSCuc47399

  Symptoms: IKEv2 STOP Accounting records show wrong counters for packets/octets, when the sessions are locally cleared using “clear crypto sa” or “clear crypto session” on ASR1K.

  Conditions: This symptom is observed with latest Cisco IOS XE Release 3.8S images when IKEV2-Accounting is enabled. This issue is easily reproducible with a single session, and may be service impacting as STOP Accounting records are usually used for billing purposes.

  Workaround: The STOP records reflect the right counters when the disconnect is through the remote-end.

- CSCuc48211

  Symptoms: Traffic from the Label Edge Router (LER) is dropped at the Label Switch Router (LSR) peer. LER is using a invalid/outdated label, unknown to LSR. This issue can be seen with a regular MPLS connection over a physical interface or with a connection over an MPLS TE tunnel interface. The root cause is that LER is using CEF long-path extension, installed to the prefix by a different routing protocol in the past.

```
TUNNEL-HEADEND/LER#show ip cef 172.25.0.1 internal
172.25.0.0/16, epoch 6, flags rib only nolabel, rib defined all labels, RIB[B],
refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00018000
   Broker: linked, distributed at 4th priority
   LFD: 172.25.0.0/16 0 local labels
        contains path extension list
  ifnums:
   TenGigabitEthernet1/0/0(31): 10.10.243.48
   Tunnel11(38)
  path 1F13EC1C, path list 1436FC80, share 1/1, type recursive, for IPv4
  recursive via 10.10.254.3[IPv4:Default], fib 21B2A5CC, 1 terminal fib,
v4:Default:10.10.254.3/32
    path 13A71668, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label 1683
    nexthop 10.10.243.48 TenGigabitEthernet1/0/0 label 1683, adjacency IP adj
out of TenGigabitEthernet1/0/0, addr 95.10.243.48 20BCED00
    path 13A745A8, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label 623
      MPLS long path extensions: MOI flags = 0x1 label 18
    nexthop 10.10.255.130 Tunnel11 label 18, adjacency IP midchain out of
Tunnel11 22923160
  long extension for path if Tunnel11 next hop 10.10.255.130:
    MPLS long path extensions: MOI flags = 0x1 label 18
  long extension for path if Tunnel22 next hop 10.10.255.129:
```

```
    MPLS long path extensions: MOI flags = 0x1 label 651
  output chain:
    loadinfo 212F8810, per-session, 2 choices, flags 0083, 4 locks
    flags: Per-session, for-rx-IPv4, 2buckets
    2 hash buckets
      < 0 > label 1683 TAG adj out of TenGigabitEthernet1/0/0, addr
10.10.243.48 20BDC860
      < 1 > label 18 TAG midchain out of Tunnel11 20C92B00 label implicit-null
TAG adj out of TenGigabitEthernet1/0/1, addr 10.10.243.50 20B21440
    Subblocks:
     None

TUNNEL-TAILEND/LSR# sh mpls forwarding-table labels 18
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
TUNNEL-TAILEND#
```

Conditions: This symptom occurs when the prefix is learned by both BGP and IGP, while BGP has lower Administrative Distance, pointing via the MPLS TE tunnel carrying MPLS. This issue is seen once the prefix is installed to RIB by IGP and then by BGP (Reload, BGP flap, etc.); then, the CEF will keep using the IGP/LDPs label without updating it in case of LDP label change.

Workaround: Issue the **clear ip route** *prefix mask* command.

- CSCuc49364

  Symptoms: A discrepancy is seen between show profile flow and show metadata table.

  Conditions: This symptom is observed on SIP Re-invite.

  Workaround: There is no workaround.

- CSCuc54300

  Symptoms: The following error message is seen during a system reboot/boot:

  ```
  "Notification timer Expired for RF Client: Redundancy Mode RF(5030)"
  ```

  Conditions: This symptom occurs during a system reboot/boot.

  Workaround: There is no workaround. This is a rare bug which needs a specific timing sequence to occur. The system reloads after this error. In most cases, the system will come up smoothly after a reload, else it will come up after one or two reloads.

- CSCuc55346

  Symptoms: SNMP MIB cbQosCMDropPkt and cbQosCMDropByte report 0.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)S1 and Cisco IOS Release 15.2. This issue is not seen with Cisco IOS Release SRE4.

  Workaround: Use SNMP MIB cbQosPoliceExceededPkt and cbQosPoliceExceededByte.

- 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).
  4. Configure IPv6 static route via the interface configured in item 3, (for example IPv6 route 2001:192:14:1::/64 2001:192:44:1::1).

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.

- CSCuc60297

  Symptoms: Redistribute or source (network statement) VRF route into BGP. BGP VRF prefix with next hop from global, the next-hop will be inaccessible.

  Conditions: This symptom is observed when redistribute VRF routes into BGP with global NH.

  Workaround: There is no workaround.

- CSCuc67687

  Symptoms: With a rare combination, and VRF-related RG configurations, the router may crash following the configuration commands.

  Conditions: This symptom is observed with the following configuration:

```
R1-13RU(config-if)#ip vrf forwarding b2b-vrf
% Interface GigabitEthernet0/1/0 IPv4 disabled and address(es) removed due to
enabling VRF b2b-vrf
% Interface GigabitEthernet0/1/0 virtual IP address <ip> removed due to VRF change
% Zone security Z1 is removed due to VRF config change on interface
GigabitEthernet0/1/0

R1-13RU(config-if)#ip address <ip> <mask>
R1-13RU(config-if)#zone-member security Z1
R1-13RU(config-if)#redundancy group 1 ip <ip> exc dec 50
```

  Workaround: There is no known workaround.

- CSCuc70310

  Symptoms: RRI routes are not installed in DMAP. “reverse-route” is a configuration in the DMAP. This prevents packets from being routed through the intended interface, and hence packet loss occurs.

  Conditions: This symptom is observed when a simple reverse-route is configured in DMAP without any gateway options.

  Workaround: There is no workaround.

- CSCuc71493

  Symptoms: Significant transaction time degradation is observed when an e-mail with attachment(s) is sent from the Windows 7 client using Outlook to a server running Outlook 2010 on the Windows 2008 server and the WAN latency is low, that is, ~12ms RTT.

  Conditions: This symptom is observed when the client is Windows 7 and data is being uploaded using the MAPI protocol and the connection is being optimized by WAAS-Express.

  Workaround: Disable WAAS-Express.

- CSCuc71706

  Symptoms: Execution of the **show run** command and other commands such as **copy run start** and **show access-list** cause the router to stop for a few minutes before completing.

  Conditions: This symptom is observed with Cisco ISR G2 routers. This issue is seen only with IPV6 configured and used.

  Workaround: There is no workaround.

- CSCuc72594

  The Cisco IOS Software implementation of the IP Service Level Agreement (IP SLA) feature contains a vulnerability in the validation of IP SLA packets 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. Mitigations for this vulnerability are available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-ipsla

  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:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

- CSCuc73677

  Symptoms: RSA keys are not generated correctly.

  Conditions: This symptom occurs when you first clear the RSA keys that are already generated on the router, and then generate the RSA keys.

  Workaround: There is no workaround.

- CSCuc76130

  Symptoms: IPsec SAs are not getting deleted even after removing the ACL.

  Conditions: This symptom occurs when using the IPsec feature with Cisco IOS Release 15.3(0.18)T0.1.

  Workaround: There is no workaround.

- CSCuc77704

  Symptoms: The GETVPN/GDOI Secondary Cooperative Key Server (COOP-KS) does not download the policy (that is, when the **show crypto gdoi ks policy** command is issued on the Secondary COOP-KS and the command output shows that no policy is downloaded) and Group Members (GMs) registering to the Secondary COOP-KS fail to register without any warning/error message.

  Conditions: This symptom is observed when the GETVPN/GDOI group (with COOP configured) has an IPsec profile configured with one of the following transforms in its transform-set:

  - esp-sha256-hmac
  - esp-sha384-hmac
  - esp-sha512-hmac

  Workaround: Use esp-sha-hmac as the authentication transform instead.

- CSCuc79143

  Symptoms: The cellular  driver should handle the profile getting inactive and should bring down the cellular interface.

  Conditions: This symptom occurs when the profile is deactivated by the HA.

Workaround: Doing a “clear line” will bring down the cellular interface and restore the connection.

- CSCuc82224

  Symptoms: When a dynamic-EID host moves from one site to another, the hosts at the old site may not be able to communicate with the host that moved away.

  Conditions: This symptom occurs if the xTR at the old site had a map-cache entry for the dynamic-EID host that moved, for example, due to lig self. Then, this map-cache entry prevents communication after the dynamic-EID host moved away.

  Workaround: Clear the map-cache entry for the host prefix in question.

- CSCuc82551

  Symptoms: A Cisco ASR 1001 running Cisco IOS XE Release 3.6.2S or Cisco IOS XE Release 3.7.1S crashes with SNMP traffic.

  Conditions: This symptom is observed with SNMP polling with an IP SLA

  configuration. The crash signature is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SNMP ENGINE
  ```

  Workaround: Remove the SNMP configuration from the router or schedule the probe before polling via SNMP.

- CSCuc87208

  Symptoms: The router crashes while configuring inherit peer-session.

  Conditions: A peer-session template is inheriting from another peer-session template where the inherited template has the “ha-mode sso” configured. For example:

  ```
  router bgp 1 template peer-session ps.rmtAS.10000 remote-as 10000 exit-peer-session
  template peer-session ps.rmtAS.10000.sso inherit peer-session ps.rmtAS.10000 ha-mode
  sso exit-peer-session template peer-session ps.rmtAS.10000.sso.bfd inherit
  peer-session ps.rmtAS.10000.sso
  ```

  Workaround: There is no workaround.

- CSCud01502

  Symptoms: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud01774

  Symptoms: Under an extremely rare occurrence, a router can crash during “no router ospf <pid>” execution.

  Conditions: This symptom is observed when there is a redistribute statement configured under the OSPF process.

  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.

- CSCud03016

  Symptoms: The TCP HA connection gets closed with SSO disabled from standby.

  Conditions: This symptom is observed when the connection is initiated from a non-HA box to an HA box.

  Workaround: There is no workaround.

- CSCud03250

  Symptoms: The performance degradation was seen starting the XE37 throttle build 09/18 (BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025).

  Conditions: This symptom is observed when the user tries with BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label and the performance number is still good, but the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025 label image shows much higher performance numbers in the order of 400 seconds. This issue is seen when the user also tries with BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label.

  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”.

- CSCud03646

  Symptoms: After SSO, sometimes the repair path over the remote LFA tunnel may point to drop adjacency.

  Conditions: This symptom is a race condition that appears infrequently in an older code base.

  Workaround: Shut/no shut the interface to force recreating the tunnel.

- CSCud06180

  Symptoms: Periodically, the Cisco EHWIC-4G-LTE-V would stop passing traffic. The user would execute “test cellular 0/1/0 mod-power-cycle” to restore service.

  Conditions: This symptom is observed during temporary network outage.

  Workaround: There is no workaround.

- 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.

- CSCud08166

  Symptoms: The Cisco ASR 1000 router crashes with “Exception to IOS Thread” and the following error:

  ```
  “UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Virtual Exec”.
  ```

  Conditions: This symptom is observed when an ACL used with “ip pim rp-address” is moved from standard to extended and "no ip multicast-routing" is configured (either in global or in a mVRF). The standard ACL must be deleted and recreated as extended, for example:

  The following series of commands are necessary to trigger the crash:

  ```
  <begin-config>
  !
  ip multicast-routing
  !
  ip pim rp-address 10.200.255.42 STATIC-RP-LN-SERVER-FARMS override
  !
  no ip access-list standard STATIC-RP-LN-SERVER-FARMS
  ip access-list extended STATIC-RP-LN-SERVER-FARMS
      remark -- STATIC RP LN SERVER FARMS MCAST GROUP ACL --
      permit ip 239.255.0.0 0.0.255.255 any
      permit ip 224.0.0.0 15.255.255.255 any
  !
  !
  no ip multicast-routing
  <end-config>
  ```

  Workaround: The crash can be prevented by any of the following methods:

  1. Disassociate the standard ACL from “ip pim rp-address” before deleting the ACL. For example.

     ```
     no ip pim rp-address 10.200.255.42 STATIC-RP-LN-SERVER-FARMS override
     and then
     no ip access-list standard STATIC-RP-LN-SERVER-FARMS
     ```

  2. Do not convert a standard ACL to extended while it is still being referenced in “ip pim rp-address”. Use a new name for the new extended ACL.
  3. Do not disable multicast routing using “no ip multicast-routing”.

- CSCud17547

  Symptoms: Mismatch of mplsXCLspId CLI and SNMP value is observed.

  Conditions: This symptom is seen when snmp query is performed.

  Workaround: There is no workaround.

- 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: This symptom is observed if metric-style wide is configured for only one level on a router running both levels, and fast-reroute is configured.

  Workaround: Configure metric-style wide for both levels (by default).

- CSCud26189

  Symptom: The map cache entries are lost after RP switchover when lisp_patr is configured.

  Conditions: This symptom occurs after RP switchover.

  Workaround: There is no workaround.

- CSCud27379

  Symptoms: WS-SUP720-3B running Cisco IOS Release 12.2(33)SRE4 crashes at

  get_alt_mod after issuing “sh run int g4/13” with several trailing white spaces until the cursor stops moving.

  Conditions: This symptom occurs when you issue the **show run interface** command with trailing spaces until the cursor stops moving.

  Workaround: Do not specify trailing spaces at the end of the **show run interface** command.

- CSCud31808

  Symptoms: With the two commands configured listed under the conditions of this release note, the Cisco router might start advertising a low TCP receive window size to the TCP peer for a specific TCP transaction. The value of this receive window size becomes equal to the configured MSS value, and it will never exceed this value anymore. This might impact TCP performance.

  Conditions: This symptom happens only if the following two commands are configured on the router:

  **ip tcp mss x**

  **ip tcp path-mtu-discovery**

  Workaround: Either change the path-mtu discovery ager timeout to 0, or remove one of the two commands.

- 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.

- CSCud36113

  Symptoms: Ping fails between CE routers.

  Conditions: This symptom is observed when you configure MPLS VPN Inter-AS IPv4 BGP Label Distribution and flaps “mpls bgp forwarding” in the interface between ASBRs.

  Workaround: Removing and adding (flapping) the static routes between ASBRs resolves the issue.

- CSCud36723

  Symptoms: RPF information for IPv6 multicast mroutes is not updated when routing changes.

  Conditions: This symptom occurs when an IPv6 multicast configuration is present in the startup configuration.

  Workaround: After startup, remove all IPv6 multicast configurations, if any, and then apply the configuration as needed.

- CSCud38774

  Symptoms: The router is showing CPU utilization at 99%. LDAP seems to be hogging the CPU process.

  Conditions: This symptom is observed randomly when NTLM authentication is deployed. This issue is observed only when the server is not able to handle the churn of requests and requests are being stuck at Bind On-Going state, which can be verified with **show ldap server** *server-name* **connections**.

  Workaround: Clearing LDAP server connections by executing the **clear ldap server** *server-name* command helps in resolving this issue:

- CSCud42529

  Symptoms: The router crashes when receiving IPv6 ICMP packet.

  Conditions: This symptom is observed when ISM-VPN is used as a crypto engine. This does not occur when using an onboard crypto engine.

  Workaround: There is no workaround.

- CSCud53872

  Symptoms: After a reload on the Cisco ASR 1000 series router, several key syslogs are sent with the incorrect source address for a few seconds. Due to the wrong source address, the syslogs are dropped at the collector end.

  Conditions: This symptom is observed when the loopback interface is configured as the source address of the syslogs.

  Workaround: There is no workaround.

- CSCud65119

  Symptoms: A crash may occur while using GETVPN with fragmented IPv6 traffic.

  Conditions: This symptom occurs when IPv6 IPsec is used. This issue is triggered by fragmented IPv6 packets.

  Workaround: There is no workaround.

- CSCud67792

  Symptoms: An invalid modem is detected.

  Conditions: This symptom is observed during bootup.

  Workaround: Use Cisco IOS Release 15.2T-based images.

- CSCud74552

  Symptoms: Ping on the EHWIC-1GE-SFP-CU interface fails.

  Conditions: This symptom is observed when ISM-VPN is installed. However, it is not necessarily utilized for encryption/decryption.

  Workaround: There is no workaround.

- CSCud78618

  Symptoms: Router crashes.

  Conditions: This symptom is seen when applying IVRF configuration on IKE profile.

  Workaround: There is no workaround.

- 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.

- CSCud86082

  Symptoms: Abnormal CPUHUG is observed when doing “config replace”.

  Conditions: This symptom is observed with “config replace” in a LISP scaling configuration.

  Workaround: There is no workaround.

- CSCud86954

  Symptoms: Some flows are not added to the Flexible Netflow cache, as indicated by the “Flows not added” counter increasing in the **show flow monitor statistics** command output. “Debug flow monitor packets” shows “FNF_BUILD: Lost cache entry” messages, and after some time, all cache entries are lost. At that moment, debug starts showing “FLOW MON: ip input feature builder failed on interface couldn't get free cache entry”, and no new entries are created and exported (“Current entries” counter remains at 0).

  The following is sample output when all cache entries are lost:

```
Router#sh flow monitor FNF-MON stat
  Cache type:                                 Normal
  Cache size:                                   4096
  Current entries:                                 0
  High Watermark:                                882

  Flows added:                                 15969
  Flows not added:                             32668
  Flows aged:                                  15969
    - Active timeout      (  1800 secs)            0
    - Inactive timeout    (    15 secs)        15969
    - Event aged                                   0
    - Watermark aged                               0
    - Emergency aged                               0
```

  Conditions: This symptom occurs when all of the following are true:

  – Flexible Netflow is enabled on a DMVPN tunnel interface.
  – Local policy-based routing is also enabled on the router.
  – Local PBR references an ACL that does not exist or an ACL that matches IPsec packets.

  Workaround: Make sure that the ACL used in the local PBR route-map exists and does not match IPsec packets sent over the DMVPN tunnel interface.

- CSCud94313

  Symptoms: PKI_INV_SPI messages are seen on the console.

  Conditions: This symptom occurs in a FlexVPN setup where Virtual-template is configured and IPsec drops are seen.

  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.

- CSCue36197

  Symptoms: A Cisco IOS 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.

- CSCue46590

  Symptoms: HTTP POST messages may not be fixed properly after adding scansafe headers.

  Conditions: This symptom was first identified on a Cisco ISR running a Cisco IOS Release 15.2(4)M2 image. A Cisco IOS Release 15.2(4)M1 image does not show the problem.

  Workaround: Whitelist the domain from being sent over to the towers.

- CSCue76102

  Symptoms: Redistributed internal IPv6 routes from v6 IGP into BGP are not learned by the BGP neighboring routers.

  Conditions: This symptom occurs because of a software issue, due to which the internal IPv6 redistributed routes from IGPs into BGP are not advertised correctly to the neighboring routers, resulting in the neighbors dropping these IPv6 BGP updates in inbound update processing. The result is that the peering routers do not have any such IPv6 routes in BGP tables from their neighbors.

  Workaround: There is no workaround.

# Open Caveats—Cisco IOS Release 15.3(1)T

All the caveats listed in this section are open in Cisco IOS Release 15.3(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtc38922

  Symptoms: A router crashes when “ip inspect” is configured.

  Conditions: This symptom is observed when “ip inspect” is configured.

  Workaround: Disable “ip inspect”.

- CSCtf50867

  Symptoms: The router reloads at iprouting_is_hdvrf_idb.

  Conditions: This symptom is observed when configuring “pri-group nfas_d” with Cisco IOS Release 15.1(01.05)T.

  Workaround: There is no workaround.

- CSCtg22670

  Symptoms: Cisco 2900/3900 routers do not detect spurious memory accesses.

  Conditions: This symptom occurs when a bug is present that causes a read from the lowest 16 KB of memory.

  Workaround: There is no workaround.

- CSCti87912

  Symptoms: While bringing up PPP sessions, server fails to add a route to the client after the IPCP negotiation happens.

  Conditions: This symptom occurs with the following two conditions:

  1. “ip unnumbered ...” per user configuration that is received from radius is applied on the virtual-access interface.
  2. Virtual-template that used for Virtual-access creation is configured with “ip unnumbered <>”.

  Workaround: There is no workaround.

- CSCtj56811

  Symptoms: After successful authorization, traffic does not pass from the IP phone or the data device.

  Conditions: This symptom is observed with the following conditions:

  - host-mode multi-domain is configured.
  - Software version: Cisco IOS Release 12.2(54)SG.

  Workaround: There is no workaround.

- CSCtj89743

  Symptoms: The Cisco Catalyst 4000 series switches running Cisco IOS Release 12.2(54)SG experiences high CPU when issuing an unsupported command, **https://ip-address**, in which ip-address is accessible from this device.

  Conditions: This symptom is observed with the Cisco Catalyst 4000 series switches.

  Workaround: There is no workaround.

  Further Problem Description: Even if SSL handshake fails, the HTTP CORE process is looping and is scheduled repeatedly.

- CSCto03904

  Symptoms: DSP is restarted when PCMU is transcoded to iLBC on DSP-SPA after “rtcp-regenerate” is enabled.

  Conditions: This symptom occurs when PCMU is transcoded to iLBC on DSP-SPA after “rtcp-regenerate” is enabled.

  Workaround: Do not enable “rtcp-regenerate”.

- CSCto08904

  Symptoms: RTP operations fail to run when using multiple operations.

Conditions: This symptom is observed when more than 16 RTP operations are running. Operations start failing due to scaling issues.

Workaround: There is no workaround.

- CSCtq23960

  Symptoms: A Cisco ISRG2 3900 series platform using PPC architecture crashes and generates empty crashinfo files:

  **show flash: all**

```
-#- --length-- -----date/time------ path
<<snip>>
2            0 Mar 13 2011 09:40:36 crashinfo_<date>
3            0 Mar 13 2011 12:35:56 crashinfo_<date>
4            0 Mar 17 2011 16:14:04 crashinfo_<date>
5            0 Mar 21 2011 05:50:58 crashinfo_<date>
```

  Conditions: This symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

  Workaround: There is no workaround.

- CSCtq36241

  Symptoms: ISG session setup fails when per-user IPv4 ACLs are used and IPv6 routing is configured.

  Conditions: This symptom is observed when both IPv6 routing and per-user IPv4 ACLs are configured.

  Workaround: Remove either IPv6 routing or per-user ACLs.

  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:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtr19078

  Symptoms: An IO memory leak in a Cisco router occurs with the following error message:

```
SYS-2-MALLOCFAIL: Memory allocation of x bytes failed
Pool: IO Alternate Pool: None Free: 0 Cause: No Alternate Pool
```

  Conditions: This symptom is observed in a Cisco 3270 router with QoS enabled. When IPsec encryption is configured on an SVI (3270 FESMIC Port) using the QoS pre-classify option, the router's memory is quickly exhausted. This happens because traffic routed out of this interface is encrypted but when the same traffic with pre-classify enabled is directed through the native Layer 3 port (MARC card ports), the Cisco 3270 router works fine.

  Workaround: Disable QoS pre-classify using the **no qos pre-classify** command.

- CSCtr39781

  Symptoms: The router hangs when it crashes at bootup.

  Conditions: This symptom occurs when the router crashes at bootup even before registry initialization.

  Workaround: There is no workaround.

Further Problem Description: If the router comes up, this issue will not occur later.

- CSCtr47084

  Symptoms: Changing the zone from the multilink interface and replacing the entire configuration by doing a **config replace flash:***config-file-name* crashes the router.

  Conditions: This symptom is observed when traffic is running.

  Workaround: There is no workaround.

- CSCtr87413

  Symptoms: Static route that is injected by “reverse-route static” in crypto map disappears when the router receives the delete notify from the remote peer. Static route also gets deleted when DPD failure occurs.

  Conditions: This symptom is observed when you configure “reverse-route static” and then receive a delete notify or DPD failure.

  Workaround: Use **clear crypto sa**.

- CSCts11166

  Symptoms: A router crashes at cce_dp_ipc_save_feature_objects.

  Conditions: This symptom occurs on a Cisco 2951 router running Cisco IOS Release 15.1(2)T1 and Cisco IOS Release 15.1(4)M1.

  Workaround: There is no workaround as the trigger of the issue is unknown.

- CSCts48300

  Symptoms: Interface queue wedge may occur when malformed traffic is received on port UDP 465. A maximum of 50 packets will become wedged.

  Conditions: This symptom occurs when some malformed traffic exists.

  Workaround: There is no know 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 4.3/3.6: 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:OF/RC:C

  CVE ID CVE-2011-4015 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

- CSCts53278

  Symptoms: Garbled voice quality with occasional periods of silence followed by a loud pop when analog STE is in secure mode with LOW line quality setting.

  Conditions: This symptom is observed with a VG224 or Cisco 2811 that is running Cisco IOS Release 15.1(4)M and connected to analog STEs with LOW line quality setting.

  Workaround: Use Cisco IOS Release 12.4(15)T14 where voice quality is still a bit garbled but there are no periods of silence or loud pops.

- CSCts86510

  Symptoms: Unable to build dIOU images.

  Conditions: This symptom is observed while compiling unused dIOU images.

  Workaround: There is no workaround.

- CSCtt29566

  Symptoms: A router running TWAMP crashes with memory corruption. This may involve a bad block pointer.

  Conditions: This symptom occurs when TWAMP is configured.

  Workaround: There is no workaround.

- CSCtu01606

  Symptoms: HWIC-2SHDSL shows no data when the controller and ATM interface are up on Alcatel and Huawei.

  Conditions: This symptom is observed with HWIC-2SHDSL when the controller and ATM interface are up on Alcatel and Huawei.

  Workaround: Reload the router.

- CSCtu02543

  Symptoms: The assigned address for an EzVPN client is not freed up after a disconnect.

  Conditions: This symptom is observed if there is another L2L tunnel terminating on the same interface of the EzVPN server.

  Workaround: There is no workaround.

- CSCtu08717

  Symptoms: A Cisco router experiences a watchdog timeout while executing tw_timer_replenish.

  Conditions: This symptom is observed on the Cisco router if the IP SLA and Performance Agent features are configured on it. This timeout may also be observed if traffic is sent for a long time through a router configured with these features.

  Workaround: There is no workaround.

- CSCtu21636

  Symptoms: Sometimes calls are dropped if there are active calls on the DSP. The following errors are displayed in the logs:

  ```
  Power alarm on DSP channel ch=1 is ON
  0001 0001 **

  Power alarm on DSP channel ch=1 is OFF
  0001 0000 **

  Power alarm on DSP channel ch=1 is ON
  0001 0001 **

  Power alarm on DSP channel ch=1 is OFF
  0001 0000 **
  ```

  Conditions: This symptom is observed with all conditions.

  Workaround: There is no workaround.

- CSCtw78539

  Symptoms: A Cisco 2901 router running Cisco IOS Release 15.2(2)T may lose dynamic routing over a Gigabit Ethernet interface.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(2)T and Cisco IOS Release 15.2(1)T1. This issue is not seen with Cisco IOS Release 15.1(4)M2 or Cisco IOS Release 15.0(1)M3.

The log may display the following:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at <snip>
reading 0x0
%ALIGN-3-TRACE: -Traceback= <snip>
%BGP-3-NOTIFICATION: received from neighbor <snip> (hold
time expired) 0 bytes
%BGP-5-ADJCHANGE: neighbor 192.168.1.1 Down BGP Notification received
%BGP_SESSION-5-ADJCHANGE: neighbor<snip> IPv4 Unicast topology
base removed from session  BGP Notification received
```

Inspection of the interface where this routing peer was established may show a lot of input/output queue drops.

Total output drops: 25185

Output queue: 331/1000/25184 (size/max total/drops)

Workaround: Reload the router or shut/no shut the interface.

- CSCtw89123

  Symptoms: A router may crash after configuring “ppp fragment delay”.

  Conditions: This symptom is observed when “ppp fragment delay” + policy-map is configured on a multilink interface and traffic crosses the device.

  Workaround: Increase “ppp multilink fragment delay” under the multilink interface and the crash will not be seen.

- CSCtx23421

  Symptoms: Leaks are seen at crypto_ceal_duplicate_pak and pak_subblock_allocate.

  Conditions: This symptom is observed when the DMVPN spoke has an IPSLA configuration and link flapping is done.

  Workaround: There is no workaround.

- CSCtx37569

  Symptoms: A BLF button (with a ephone-dn) that has been configured for park-slot turns red when a call is parked. But, sometimes, after the call has been retrieved, the button stays red and remains red until the phone restarts.

  Conditions: This symptom is observed with a BLF button (with a ephone-dn) that has been configured for park-slot.

  Workaround: Restart the phone to clear the BLF button.

- CSCtx52157

  Symptoms: SM-ES3G-24-P module installed in a Cisco 3925E chassis shows the status as failed.

  Conditions: This symptom is observed with an SM-ES3G-24-P module installed in a Cisco 3925E chassis.

  Workaround: Reload the SM-ES3G-24-P switch module.

- CSCtx56183

  Symptoms: The router crashes due to a block overrun:

  ```
  %SYS-3-OVERRUN: Block overrun at 49156754 (red zone 66616365)
  -Traceback= 42806C04z 42809B20z 42809D14z 427AD988z 427AD96Cz
  .
  .
  %SYS-6-BLKINFO: Corrupted redzone blk 49156754....
  .
  ```

```
%SYS-6-MEMDUMP: 0x49156754: 0xAB1234CD 0x12A0000 0x12C 0x44395148
%SYS-6-MEMDUMP: 0x49156764: 0x419B243C 0x49157154 0x49156658 0x800004E8
%SYS-6-MEMDUMP: 0x49156774: 0x1 0x0 0x1000133 0x47D7699C
```

Conditions: This symptom occurs when Websense URL filtering is enabled and long URLs have been accessed.

Workaround 1: Disable URL filtering.

Workaround 2: Do not invoke long URLs.

- CSCtx65384

  Symptoms: The L2TPv3 session is not reestablished when a pseudowire is configured with the loopback address and the loopback interface is deleted and readded.

  Conditions: This symptom occurs when the local interface used is a loopback interface and the loopback is removed and re-added. This issue was seen with a Cisco 2800 router loaded with Cisco IOS interim Release 15.2(1)T1.11.

  Workaround: Remove and readd the pseudowire-class after adding the loopback interface.

- CSCty09784

  Symptoms: The SS7 link does not come up.

  Conditions: This symptom is observed with the fix of DDTS CSCta18342.

  Workaround: Use the version of Cisco IOS that has the issue of “D channel is not recovering after IP flapping IUA”.

- CSCty82414

  Symptoms: A crash is seen.

  Conditions: This 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.

- CSCtz28855

  Symptoms: The router may crash after printing several error messages:

  ```
  %SYS-2-NOTQ: unqueue didn't find 87FFED94 in queue 865335D8 -Process= "IP
  Input", ipl= 0, pid= 113
  %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 87FFEDCC. -Process=
  "IP Input", ipl= 0, pid= 113
  ```

  Conditions: This symptom is observed with Cisco IOS Release 15.2(2)T1 with Trend URL Filtering configured.

  Workaround: There is no workaround.

- CSCtz54775

  Symptoms: Traffic sourced from a 2901 through an EHWIC-4ESG module resumes forwarding within a maximum of 5 minutes (ARP expiry) instead of 30 seconds (STP convergence time).

  Conditions: This symptom is observed after an STP failover.

  Workaround: Clear the ARP table of the affected interface (after the VLAN is in a forwarding state).

- CSCtz57013

  Symptoms: The Cisco UC540 crashes randomly every few weeks.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T2 and Cisco IOS Release 15.1(2)T4.

Workaround: There is no workaround.

- CSCtz57617

  Symptoms: The following logs are reported on the Cisco 1803 router randomly:

```
Apr  7 19:01:48: %C1800-3-SPIACQUIREFAIL: Failed to acquire SPI due
to internal error, spi_running 1 spi_locked 1
Apr  7 19:01:48: -Traceback= 80D928A0z 8002215Cz 8002D18Cz 8031A100z
8031D36Cz 8031D76Cz 8031E080z 8031F910z 8031C08Cz 8031C770z 8031A09Cz
80121DACz 8001B210z 8001B210z 80121E68z 80122590z
Apr  7 19:01:48: ASSERTION FAILED: file
```

  Conditions: This symptom occurs on the Cisco 1803 router.

  Workaround: There is no workaround.

- CSCtz84873

  Symptoms: A crash is observed due to stack overflow:

```
%SYS-6-STACKLOW: Stack for process CCSIP_SPI_CONTROL running low, 0/60000
```

  Conditions: This symptom is observd on a SIP gateway. The conditions are still being investigated.

  Workaround: There is no workaround.

- 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 a configuration change is needed.
  2. Remove ACL checks on the interface when changing the configuration (“no ip access-group..”).

- CSCua26981

  Symptoms: A Cisco ASR router may crash due to a CPU Watchdog upon invocation of “show ip eigrp neighbor detail”.

```
sh ip eigrp nei detail
<snip>
ASR1000-WATCHDOG: Process = Exec
%SCHED-0-WATCHDOG: Scheduler running for a long time, more than the maximum
configured (120) secs.
-Traceback= ...
========= Start of Crashinfo Collection (09:21:44 EST Wed May 9 2012) ==========
```

  Conditions: This symptom occurs when the Cisco ASR router is experiencing rapid changes in EIGRP neighborship, such as during a flap. One way to artificially create this scenario is to mismatch the interface MTU.

  Workaround: There is no workaround.

- CSCua28693

  Symptoms: One-way audio is experienced. The gateway is streaming G.729 instead of G.711 which was negotiated through SIP signaling.

  Conditions: This symptom is observed with a Cisco 2821 and Cisco IOS Release 15.1(4)M1.

  Workaround: Use G.729 instead of G.711.

- CSCua49735

  Symptoms: The WAAS-Express router crashes in HTTP-Express Accelerator.

  Conditions: This symptom occurs when HTTP-Express Accelerator is enabled and HTTP traffic is going through the WAAS-Express router.

  Workaround: Disable HTTP-Express Accelerator.

- CSCua50697

  Symptoms: After unplugging and reconnecting a T1 cable, the T1 controller remains down or report continuous errors. After a router reload, the T1 controller remains up until the cable is disconnected again.

  Conditions: This symptom affects only the following cards: HWIC-xCE1T1-PRI, NM-8CE1T1-PRI, VWIC3-xMFT-T1/E1, and GRWIC-xCE1T1-PRI.

  Also, the T1 signal must be somewhat out-of-specification according to T1.403 standards.

  Workaround 1: Reload the router with the T1 cable plugged in.

  Workaround 2:

  1. Upgrade to a fixed-in Cisco IOS version.
  2. Issue the following commands (hidden, so tab complete will not work):

```
enable
config t
controller <t1/e1> <slot/subslot/port> ! ( example: controller t1 0/0/0 )
hwic_t1e1 equalize
```

  3) Shut/no shut the T1 controller, or reload the router to allow the CLI to take effect.

- 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.

- CSCua68587

  Symptoms: cvCallVolConnActiveConnection.sip MIB count does not match what is seen on the CLI.

  Conditions: This symptom is observed with the Cisco ASR 1006 running Cisco IOS XE Release 3.6.0S or Cisco IOS Release 15.2(2)S with the asr1000rp2-adventerprisek9.03.06.00.S.152-2.S image.

  Workaround: There is no workaround.

- 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.

- CSCua76157

  Symptoms: BGP routes are displayed.

  Conditions: This symptom occurs after removing the “send-label” from PE.

  Workaround: There is no workaround.

- CSCua92741

  Symptoms: Remote neighbors are denied by the allow-list to come up.

  Conditions: This symptom occurs when the remote neighbor is configured with a /32 IP address.

  Workaround: There is no workaround.

- CSCub10239

  Symptoms: ATM PVC on the Cisco 887M router does not restore itself, if the interface is bounced.

  Conditions: This symptom is observed with Cisco IOS versions apart from Cisco IOS Release 15.0(1)M.

  Workaround: Reboot the router.

- CSCub18622

  Symptoms: Dynamic ACL does not get applied to the interface ACL, but the user shows up in the **show ip auth-proxy cache** command output.

  Conditions: This symptom occurs when auth proxy is configured on a tunnel interface.

  Workaround: Move the auth-proxy rules onto a physical interface.

- 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.

- CSCub19185

  Symptoms: Path confirmation fails for a SIP-SIP call with IPV6 enabled.

  Conditions: This symptom occurs when UUTs are running Cisco IOS Release 15.2(2)T1.5.

  Workaround: There is no workaround.

- CSCub21128

  Symptoms: The “cns id udi”-related configuration does not get loaded into running-configuration on the Cisco 1900 router.

  Conditions: This symptom is observed when the UDI on the Cisco 1900 router is unavailable during the device startup time.

  Workaround: Reconfigure “cns id udi” later.

- CSCub33087

  Symptoms: The router crashes at QOS on the ATM subinterface.

  Conditions: This symptom occurs during normal operations at the customer site.

  Workaround: There is no workaround.

- CSCub33602

  Symptoms: IGMP query with source IP address 0.0.0.0 triggers a querier election process. As a consequence, port on which this packet is received is marked as mrouter port for that VLAN.

```
Router#show ip igmp int vlan 1
Vlan1 is up, line protocol is up
  Internet address is 1.1.1.1/24
  IGMP querying router is 0.0.0.0 <----

Router#sh ip igmp snooping mrouter
vlan            ports
-----+---------------------------------------
   1  Po1,Po8,Router<-----
```

  Conditions: This symptom is observed when IGMP query with source IP address 0.0.0.0 is received.

Workaround: Configure an ACL to block packets with source IP address 0.0.0.0 and apply it to relevant interfaces.

```
access-list 100 deny   ip host 0.0.0.0 any
    access-list 100 permit ip any any
    int vlan 1
     ip access-group 100 in
```

Further Problem Description: Per RFC 4541, IGMP query with source IP address 0.0.0.0 is used in special cases. When such query is received by a router, it should not be used in the querier election process.

- CSCub34396

  Symptoms: Because of the fix for CSCtw52819, non-NHRP process switched packets are noticed to go as clear text.

  Conditions: This symptom is observed with a DMVPN configuration.

  Workaround: There is no workaround.

- CSCub34534

  Symptoms: A basic call between 2 SIP phones over SIP trunk (KPML-enabled) fails.

  Conditions: This symptom is observed with Cisco ISR G2 platforms.

  Workaround: There is no workaround.

- CSCub36684

  Symptoms: Slow memory leak is observed.

  Conditions: This symptom occurs due to the SNMP engine.

  Workaround: There is no workaround.

- CSCub45054

  Symptoms: OQD drop counters increment on the mGRE tunnel even though there are no drops.

  Conditions: This symptom is observed with an mGRE tunnel when multicast traffic is sent over the tunnel. This issue is seen when EIGRP or OSPF is configured on the tunnel.

  Workaround: There is no workaround.

- CSCub45632

  Symptoms: Ping failure occurs after modem-reset and sweep-ping is not intermittent.

  Conditions: This symptom occurs after loading the router with the Cisco IOS Release 15.2(4)M1 image.

  Workaround: There is no workaround.

- CSCub52825

  Symptoms: The negotiated global IPv6 remains intact on the Dialer interface.

  Conditions: This symptom is observed when the physical interface goes down.

  Workaround: Remove the global IPv6 address manually from the Dialer interface.

- CSCub53380

  Symptoms: Legitimate PPP frames are dropped on an async interface, incrementing both “runts” and “unknown protocol drops” in the <CmdBold>show interfaces<noCmdBold> command.

  Conditions: This issue is observed with Cisco ISR G1/G2 platforms running Cisco IOS Release 15.x with the following modules.

  - HWIC-4A/S
  - HWIC-8A/S-232
  - HWIC-8A
  - HWIC-16A

  Workaround: There is no workaround.

- CSCub55303

  Symptoms: HWIC-4ESW stops passing the traffic after 5-6 days of operation on Cisco 2911/K9 running Cisco IOS Release 15.2(3)T1.

  Conditions: This symptom is observed with Cisco 2911/K9 running Cisco IOS Release 15.2(3)T1.

  Workaround: Shut/no shut on the HWIC interface restores connectivity.

- CSCub56064

  Symptoms: Ping fails after doing EZVPN client connect if CEF is enabled.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(0.8)T image. This issue is seen only for a specific topology, where the in/out interface is the same.

  Workaround: There is no workaround.

- CSCub56842

  Symptoms: The router stops passing IPsec traffic after some time.

  Conditions: This symptom is observed when the **show crypto eli** command output shows that during every IPsec P2 rekey, the active IPsec-Session count increases, which does not correlate to the max IPsec counters displayed in SW.

  Workaround: Reload the router before active sessions reach the max value.

  To verify, do as follows:

```
router#sh cry eli

 CryptoEngine Onboard VPN details: state = Active
 Capability    : IPPCP, DES, 3DES, AES, GCM, GMAC, IPv6, GDOI, FAILCLOSE, HA

 IPSec-Session :  7855 active,  8000 max, 0 failed <<<
```

- CSCub58146

  Symptoms: There is an inconsistency in how NM-16ESW@C2821 handles unregistered multicast groups with IGMP Snooping. It is expected with Cisco IOS is that those groups will be flooded. However, what is observed is that in some VLANs, unregistered groups are flooded and in other VLANs, they are not. Behavior also changes between node reloads and VLAN delete and add (stops flooding). RFC4541 also explicitly requires configuration knob per-interface to enable flooding. On other platforms, this is done by using the **switchport block multicast** command. Cisco C2821 lacks this functionality. An unregistered packet is defined as an IPv4 multicast packet with a destination address that does not match any of the groups announced in earlier IGMP Membership Reports. If a switch receives an unregistered packet, it must forward that packet on all ports to which an IGMP router is attached. A switch may default to forwarding unregistered packets on all ports. Switches that do not forward unregistered packets to all ports must include a configuration option to force the flooding of unregistered packets on specified ports.

  Conditions: This symptom is observed with the following conditions:

  - The L2 access port located at NM-16ESW is receiving IPv4 multicast traffic.

  - Cisco IOS Release 12.4(25a), Cisco IOS Release 15.1(4)M4, and Cisco IOS Release 15.0(1)M8.

  Workaround: There is no workaround.

- CSCub61009

  Symptoms: Spurious errors are observed on the Cisco AS5400.

  Conditions: This symptom is observed on the Cisco AS5400 .

  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 6.8/6.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C

  CVE ID CVE-2012-5422 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

- CSCub61795

  Symptoms: The log fills with SYS-2-BADSHARE messages, leading to a crash.

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=69AD4440, count=0
      -Traceback= 601E887Cz 601E50B4z 601E56C0z 602D24CCz 60F38F04z 6065B628z
       Invalid magic number in receive buffer (0x0)
  ```

  Conditions: This symptom occurs with a large amount of traffic passing through an ATM interface. This issue might be specific to an ATM interface using the CX27470 ATMOC3 driver as seen in the **show interface** command output. The ATM module that the issue was originally seen on was a NM-1A-OC3-POM. QOS might be needed to trigger the issue.

  Workaround: A possible but unconfirmed workaround is to disable QOS on the interface.

- CSCub65620

  Symptoms: Packets being replicated to snoop is taking more time. The calls are also getting successes.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 15.3(01.02)T with the Linux server.

  Workaround: There is no workaround.

- CSCub65760

  Symptoms: MSP is failing to populate the **show profile flow** command on the Cisco ISR G2 for a SIP call made from a connected video endpoint.

  Conditions: This symptom is observed when the connected endpoint is registered to the call manager and makes a SIP call to another video endpoint. The SIP OK message returning from the call manager is segmented.

  Workaround: There is no workaround.

- CSCub66367

  Symptoms: When using HWIC-2SHDSL with "ppp mulitlink fragment" configured, there is some packet loss when pings are sourced from a PC. But, when pings are sourced from the router, there is no ping loss. When "ppp mulitlink fragment" is not configured, no ping loss is experienced even when pinging from the PC.

  Conditions: This symptom occurs when "ppp mulitlink fragment" is configured.

Workaround: There is no workaround.

- CSCub69270

  Symptoms: Latency is observed in VPN traffic. Packet drops may also be seen.

  Conditions: This symptom occurs when the ISM VPN module is enabled.

  Workaround: Disable the ISM module.

- 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”.

- CSCub74272

  Symptoms: Intermittently during Phase II rekey, after new SPIs are negotiated and inserted into SPD, old SPIs are removed and then the VTI tunnel line protocol goes down.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T, with VTI over GRE.

  Workaround: There is no workaround.

- CSCub74692

  Symptoms: Path confirmation fails while making H.323 calls in IEC_FORCED_DISENGAGE,IEC_GK_SHUTDOWN and Long call detection scenarios.

  Conditions: This symptom is observed while making H.323 calls in IEC_FORCED_DISENGAGE,IEC_GK_SHUTDOWN and Long call detection scenarios.

  Workaround: Disable CEF using the **no ip cef** command in the GW configuration.

- CSCub79318

  Symptoms: Codec changes spontaneously during midsession without a RE-INVITE.

  Conditions: This symptom occurs with the following conditions:

  - Fax passthrough is configured.
  - Codec negotiated is G711alaw, and changes to G729.

  Workaround: There is no workaround.

- CSCub80386

  Symptoms: The following interface configuration should be used:

  ```
  interface Ethernet2/1
  description lanethernet1
  ipv6 enable
  ospfv3 100 network manet
  ospfv3 100 ipv6 area 0
  ```

  Dead interval is calculated according to network type; in this case, it is 120s. Issue the **no ospfv3 dead-interval** command on dead interval. Dead interval is set to the default of 40s instead of 120s, which is correct for manet or P2MP interface types.

  Conditions: This symptom is an OSPFv3-specific issue (see the configuration example).

  Workaround: Configure dead interval explicitly or reapply the network command.

- CSCub80654

  Symptoms: Randomly, there is no audio if a call comes from the following call flow using G729:

  ```
  IP Phone -- CUCM -- ICT GK Controlled -- GK -- CME 9.1 -- Phone A and B
  ```

  If one of the phones in CME tries to GPickup the call randomly, it will have no audio. When this happens, if you check the codec directly in the phone, it is G711. However, when it works, it is G729. Everything is configured for G729. Even if you hardcode the phone in CME to use G729, this issue will occur. This issue does not occur in CME 7.1.

  Conditions: This symptom occurs if a call comes from GK as G729 and CME 9.1 is being used.

  Workaround: Use CME 7.1 or enable fast start in CUCM Trunk by enabling the following check boxes:

  - Media Termination Point Required
  - Enable Outbound FastStart
  - Codec For Outbound FastStart ? G729

  Also, configure Cisco IOS MTP to use G729.

- CSCub80710

  Symptoms: SSL handshake between Cisco VCS and the Cisco ASR fails if the Cisco ASR is running Cisco IOS XE Release 3.7S.

  Conditions: This symptom occurs in a working setup, if the Cisco ASR is upgraded to Cisco IOS XE Release 3.7S, then SSL handshake and subsequently SIP-TLS calls start to fail. If in the same setup, the Cisco ASR is downgraded back to Cisco IOS XE Release 3.5S or Cisco IOS XE Release 3.4.4S, then the calls work (without requiring any additional changes).

  Workaround: There is no workaround.

- CSCub82495

  Symptoms: Channel-group goes down with the HWIC-xCE1T1-PRI controller after reloading the router.

  Conditions: This symptom occurs when channel-group goes down after reload.

  Workaround: There is no workaround.

- CSCub83371

  Symptoms: Performance degradation with high CPU is seen on CUBE for SIP-SIP flow-through calls.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(1)T2.13.

  Workaround: There is no workaround.

- CSCub85451

  Symptoms: When Scansafe is enabled on the interface, latency may be seen. Some pages may not load at all or show severe latency if the SYN request sent by the Cisco ISR does not receive an appropriate SYN ACK response from the Scansafe Tower.

  Conditions: This symptom occurs when Scansafeis enabled on the interface. In this case, there was an ASA in the path that was doing sequence number randomization.

  Workaround: Disable sequence number randomization on the firewall in the path before the Cisco ISR.

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-2012-4651 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

- CSCub86011

  Symptoms: The embedded event manager (EEM) is not available on the Cisco VG202/204.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T or later releases.

  Workaround: There is no workaround.

- CSCub86574

  Symptoms: The router crashes if PfR and EIGRP are configured on the router.

  Conditions: This symptom is observed with four exit interfaces, that is, two per BR.

  Workaround: There is no workaround.

- CSCub89144

  Symptoms: The VTI tunnel is always in up/up state.

  Conditions: This symptom is observed when HSRP failover is configured on the HSRP standby router only. This issue was first seen on the Cisco ASR router, but it is platform-independent and is seen on the latest Cisco IOS Release 15M&T and later releases as well.

  Workaround: Use GRE or routing protocols for redundancy.

- CSCub90414

  Symptoms: The device crashes when a block of memory is freed, even though it was not in use.

  Conditions: This symptom occurs when "crypto pki trustpoint" is configured.

  Workaround: Remove the **auto-enroll** command to prevent any other reloads due to this bug. The ultimate resolution is to upgrade Cisco IOS to a release that contains the fix for this bug.

- CSCub95261

  Symptoms: The device crashes due to a bad reference count.

```
%SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count, chunk 40A82BB4 data
313E2F40 refcount FFFFFFFF alloc pc
    2341E7F4. -Process= "CSDB Timer process", ipl= 3, pid= 274
    -Traceback= <HEX TRACEBACK HERE>

    chunk_diagnose, code = 3
    chunk name is CSDB l4 structu

    current chunk header = 0x313E2F30
    data check, ptr = 0x313E2F40

    next chunk header = 0x313E2F90
    data check, ptr = 0x313E2FA0

    previous chunk header = 0x313E2ED0
    data check, ptr = 0x313E2EE0
```

  Conditions: This symptom is still being investigated. The exact conditions are unknown. However, this issue is known to occur when IPS is enabled.

Workaround: There is no workaround.

- CSCub96176

  Symptoms: The router crashes when the DNS server is turned on.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M1.

  Workaround: There is no workaround.

- CSCub98623

  Symptoms: The **show int** command output displays the input queue size as bigger the 0, and never goes down. Shut/no shut does not help as well.

  Conditions: This symptom is observed with the following conditions:

  – A Cisco IOS router actions as XOT.

  – The XOT Server becomes not reachable for sometime while the x25 client is attempting to send traffic.

  – Cisco IOS Release 12.4(24)T7, Cisco IOS Release 15.1M, or later releases.

  Workaround: Increase the input hold queue size from default 75 to max. Monitor it periodically manually or by script and perform a planed reload when the queue size is close to max.

- CSCuc02262

  Symptoms: A crash is seen at tcp_prepare_for_retransmit with the combination of IPv6 and IPv4 traffic.

  Conditions: This symptom is observed in a DMVPN setup with the Cisco 2921 acting as the spoke and the Cisco 3945e as the hub. After passing HTTP traffic using IPv4 as well as IPv6, a crash is seen on the spoke.

  Workaround: There is no workaround.

- CSCuc07669

  Symptoms: CPU utilization is more under DoS attack using L2TPv3 packets in Cisco IOS Release 15.0M.

  Conditions: This symptom is observed with Cisco IOS Release 15.0M only with DoS attacks triggered with L2TPv3 packets.

  Workaround: There is no workaround.

- CSCuc07984

  Symptoms: The Cisco 819 router serial interface does not interoperate with modems such as Adtran, Aethra,and Pardayn.

  Conditions: This symptom occurs on the serial interface on the Cisco 819 series router while connecting to some specific types of modems.

  Workaround: There is no workaround.

- CSCuc09559

  Symptoms: A crash is seen on a Cisco 3900e router running Cisco IOS Release 15.2(2)T when adding a new crypto peer. The device crashes when making configuration changes to add the peer.

  The crash is of the following type:

```
SYS-2-CHUNKBADFREEMAGIC  Bad free magic number in chunk header
In the
"SADB Peering Ch" chunk
```

Conditions: This symptom occurs when making configuration changes to add the crypto peer.

Workaround: There is no workaround.

- CSCuc10588

  Symptoms: The router crashes.

  Conditions: This symptom occurs when the normalizer engine is running with the traffic being sent.

  Workaround: There is no workaround.

- CSCuc12365

  Symptoms: With the ISM module enabled, the tunnel comes up but the OSPF adjacency does not come up, hence no traffic passes. The tunnel shows up without passing traffic for approximately 20 minutes, and after that, the outside interface becomes unresponsive and the SAs go down. Reboot is the only way to bring it back up. A traceback may also be seen.

  Conditions: This symptom occurs when the ISM module is being used on Cisco IOS Release 15.2(3)T1 or later releases.

  Workaround: Disable the ISM module.

- CSCuc12685

  Symptoms: A router has an unexpected reload in SIP code.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M4.

  Workaround: There is no workaround.

- CSCuc14088

  Symptoms: The default class is not being exported with the class option template.

  Conditions: This symptom occurs when class-default is not exported when typing the option c3pl-class-table under the flow exporter.

  Workaround: 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.

  Workaround 1: Disable CEF.

  Workaround 2: Do not configure “ip traffic-export” in the crypto map interface.

  Workaround 3: Disable ISM using “no cry engine slot 0”. Then, the onboard engine will be used.

- CSCuc16172

  Symptoms: When the reset button is pushed on a Cisco C881W-A-K9 router, the start-up configuration is automatically backed up as “startup.backup.xxx” and stored in the flash.

  Conditions: This symptom occurs when a xxx.cfg file is present on the flash and the push button is pressed. The Cisco C881W-A-K9 Router boots up with the xxx.cfg file present on the flash, but also backs up the start-up configuration as “startup.backup.xxx” and stores it on the flash.

  Workaround: There is no workaround.

- CSCuc18606

  Symptoms: After BGP flap or device reload, the following error is displayed in the log:

  ```
  BGP-3-DELROUTE  Unable to remove route for [XYZ] from radix trie
  ```

  There is also a reachability issue.

  Conditions: This symptom is observed during BGP flap, router reload, and when changing the NET statement under the ISIS process.

  Workaround: Reconfiguring NET under ISIS or reloading the device may help to resolve the issue.

- CSCuc19520

  Symptoms: The Cisco ISR by default allocates the first available free port in case of port collision. Due to this, there are chances of frequent reuse of the same ports that can potentially lead to some issues.

  Conditions: This symptom occurs when Cisco ISR by default allocates the first available free port in case of port collision.

  Workaround: This bug is not a functionality impacting bug. However, having this fix will reduce other complications.

- CSCuc19800

  Symptoms: The router crashes.

  Conditions: This symptom occurs when the **no switchport** command is issued under the UCSE x/1 interface.

  Workaround: There is no workaround.

- CSCuc21859

  Symptoms: Memory leak is seen at ssf_owner_get_feature_sb.

  Conditions: This symptom occurs when the discriminator configuration is with logging, as given in the below examples:

  ```
  logging discriminator <NAME>
  logging host x.x.x.x discriminator DEBUG
  logging discriminator SysLog mnemonics drops NAME
  ```

  Workaround: Remove the discriminator configuration from the logging configuration.

- CSCuc23863

  Symptoms: Traffic is dropped over the tunnel when it hits multiple zone Cisco IOS FW.

  Conditions: This symptom is observed with the following conditions:

  1. ZBFW with three or more zones.
  2. Self-zones defined.
  3. DVTI configured.
  4. Hairpins traffic.

  Workaround:

  1. Configure only two zones.
  2. Disable self-zones.
  3. Disable CEF.

4. Allow the same traffic in the outside-to-inside policy to whatever is allowed in inside-to-outside.

- CSCuc24189

  Symptoms: A Cisco NHRP router may unexpectedly reload at function rn_match.

  Conditions: This symptom occurs when the router is running NHRP and the NHRP SNMP MIB is enabled.

  Workaround: A possible workaround is to disable the NHRP SNMP MIB. Save the configuration and reload the router. This needs to be confirmed with development after the bug is fixed.

- CSCuc25634

  Symptoms: WAAS-optimized traffic gets dropped by ZBFW HA.

  Conditions: This symptom occurs when ZBFW HA and SRE-WAAS are configured.

  Workaround: There is no workaround.

- CSCuc26021

  Symptoms: The crypto IKEv2 session is shown as active when the VA interface goes down for a spoke-to-spoke FlexVPN.

  Conditions: This symptom occurs when the traffic is running and when crypto engine is switched from onboard crypto to software crypto.

  Workaround: There is no workaround.

- CSCuc30438

  Symptoms: Capturing the passwords in plain text is possible via the EEM CLI ED option.

  Conditions: This symptom occurs when an applet is written to capture the CLIs(_cli_msg) and redirect it to a file.

  Workaround: There is no workaround.

- CSCuc30630

  Symptoms: An update to the Cisco IOS-IPS signature package may cause the router to crash in some very rare scenarios, when signature scanning and signature build happens simultaneously.

  Conditions: This symptom occurs on a Cisco 2911 ISR G2 router running Cisco IOS Release 15.2(4)M1.

  Workaround: There is no workaround.

- CSCuc30836

  Symptoms: Cisco IOS IPS signature auto-updates fail.

  Conditions: This symptom occurs on a Cisco c880 router running Cisco IOS Release 15.1(4)M4 on signature definition S636.

  Workaround: There is no workaround.

- CSCuc31371

  Symptoms: The IKEv2 session is shown as up for a Spoke-to-Hub FlexVPN.

  Conditions: This symptom occurs when the tunnel interface is shut down.

  Workaround: There is no workaround.

- CSCuc31725

  Symptoms: CUBE fails to resolve the configured DNS through A query when the SRV query fails.

Conditions: This symptom occurs when running Cisco IOS Release 15.3(0.11)T.

Workaround: Use DNS SRV records for SIP servers.

- CSCuc32663

  Symptomx: User passwords appear in ACS logs.

  Conditions: This symptom occurs on a device running Cisco IOS software configured with AAA TACACS configuration command authorization, will transit the user password as entered in any configuration CLI command that requires both the username and password in the command authorization AVs as part of the command authorization request.

  Example of CLI commands: **username** *name* **password** *password*

  The *password* is sent as part of the data for configuration command authorization.

  Workaround: Disable the configuration command authorization.

  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:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc33119

  Symptoms: WAAS-optimized traffic may get stuck in a loop when ISM VPN is enabled.

  Conditions: This symptom occurs only when the ISM VPN module is turned on.

  Workaround: There is no workaround.

- CSCuc33436

  Symptoms: After a reload, the first incoming PRI call fails to connect. Subsequent calls work fine.

  Conditions: This symptom is observed when using PVDM2-xDM and HWIC-xCE1T1-PRI for data PRI calls on Cisco IOS Release 15.2(3)T.

  Workaround: Run "clear modem all" after a reload.

- CSCuc34107

  Symptoms: The shaper does not work.

  Conditions: This symptom does not occur under any specific conditions.

  Workaround: There is no workaround.

- CSCuc38552

  Symptoms: On SS0, traffic is not resumed within a second and packet loss is seen in EoMPLS port.

  Conditions: This symptom occurs on SSO.

  Workaround: There is no issue in the release branch "mtrose". This issue is seen on the child branch "ma3_gcc421_compiler".

- 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: This symptom is observed when Cisco IOS CUBE experiences an input queue wedge condition on an interface configured for media negotiation using SIP when a 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

- CSCuc42558

  Symptoms: A Cisco router configured as the VXML gateway may experience a leak in the processor memory pool in CCSIP_SPI_CONTROL in the function url_parseTelUrl.

  Conditions: This symptom occurs when a Cisco router is configured as the VXML gateway.

  Workaround: Reload the router during a maintenance window to avoid an unexpected crash. You may also downgrade to Cisco IOS Release 15.1(4)M3, which is not affected.

- CSCuc44438

  Symptoms: There is a memory corruption issue with loading NBAR protocol pack.

  Conditions: This symptom occurs when an NBAR protocol pack is loaded into the router using the **ip nbar protocol-pack** command.

  Workaround: There is no workaround.

- CSCuc44629

  Symptoms: The switch/router crashes while processing NTP.

  Conditions: This symptom occurs if NTP is configured using DNS, along with the source interface. For example:

  ```
  config# ntp server <dns> source <interface>
  ```

  Workaround 1: config# ntp server <dns>

  Workaround 2: config# ntp server <ip>

  Workaround 3: config# ntp server <ip> source <interface>

  For workarounds 1 and 2, the device automatically selects the source interface. For workarounds 2 and 3, resolve the DNS and use the corresponding IP address for that DNS.

  For example:

  ```
  Router# ping <dns>
  ```

  The above command gives the IP address for DNS. Use that IP address to configure the NTP server.

- CSCuc45045

  Symptoms: The **show ip eigrp neighbors detail vmi** command displays large delay values.

  Conditions: This symptom is observed only for the VMI interface in MANET networks.

  Workaround: There is no functional impact because of this. For any other practical purposes, convert the displayed value from pico second to microsecond as the value displayed is in pico seconds and units displayed are in usec.

- CSCuc45528

  Symptoms: Incremental leaks are seen at :__be_nhrp_recv_error_indication.

  Conditions: This symptom occurs when the NHRP error indication is received on the box. This issue is seen only if CSCub93048 is already present in the image. CSCub93048 is available from Cisco IOS Release 15.3M&T onwards.

  Workaround: There is no workaround.

- CSCuc46087

  Symptoms: CUBE does not send a response to an early dialog UPDATE in a glare scenario.

  Conditions: This symptom occurs when CUBE receives an early dialog UPDATE when it sends 200OK to INVITE and expects ACK.

  Workaround: There is no workaround.

- CSCuc47036

  Symptoms: A crash occurs due to memory corruption pointing to TCP/BGP functions.

  Conditions: This symptom occurs when eBGP is configured and the link is flapped.

  Workaround: There is no workaround.

- CSCuc47356

  Symptoms: Static routes are not getting removed.

  Conditions: This symptom is observed with Smap - Smap. Removal of CLI does not remove the static route.

  Workaround: Remove the ACL before removing the SA.

- CSCuc47399

  Symptoms: IKEv2 STOP Accounting records show wrong counters for packets/octets, when the sessions are locally cleared using “clear crypto sa” or “clear crypto session”.

  Conditions: This symptom is observed with latest Cisco IOS XE Release 3.8S images when IKEV2-Accouting is enabled. This issue is easily reproducible with a single session, and may be service impacting as STOP Accounting records are usually used for billing purposes.

  Workaround: The STOP records reflect the right counters when the disconnect is through the remote-end.

- CSCuc49335

  Symptoms: An infinite loop is seen at tunnelInetConfigIfIndex.ipv6 while doing SNMP walk.

  Conditions: This symptom occurs when an SNMP walk is done on the Cisco ISRG2 router and the Cisco ASR 1000 router.

  Workaround: There is no workaround.

- CSCuc49364

  Symptoms: The Media-service Proxy table gets populated but the Metadata table does not get populated.

  Conditions: This symptom is observed in Cisco ISR platforms.

  Workaround: There is no workaround.

- CSCuc51617

  Symptoms: Poor video quality is observed.

Conditions: This symptom occurs at the beginning of the call. This issue occurs because of some missing configurations at the dial peer.

Workaround: The quality improves after hold and resume.

- CSCuc51774

  Symptoms: Packet drop is seen on the 4G/LTE cellular interface when QoS is configured with the parent shaper.

  Conditions: This symptom is observed QoS with the parent shaper enabled on the 4G/LTE interface.

  Workaround: Remove QoS or use QoS without the shaper.

- CSCuc52038

  Symptoms: CUBE is configured with media antitrombone. A call is made from PSTN ---> CUBE and forwarded to another PSTN phone. There is only one-way media from the called device to the calling device. When media antitrombone is disabled, there is media flow both ways. This behavior is seen only when media antitrombone is enabled in CUBE. Please check for enclosures for debug ccsip all messages of both CUBE and the PSTN router.

  Conditions: This symptom occurs when media antitrombone is enabled.

  Workaround: Disable media antitrombone.

- CSCuc52757

  Symptoms: The encrypt and decrypt packet count does not match.

  Conditions: This symptom is observed with encrypt and decrypt packets.

  Workaround: There is no workaround.

- CSCuc55407

  Symptoms: The following error message is displayed:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle error logs followed by traceback
  ```

  Conditions: This symptom is observed with STM flapping and a badshare alarm.

  Workaround: There is no workaround.

- CSCuc58194

  Symptoms: While configuring the channelized interfaces, SNMP-related tracebacks are seen.

  Conditions: This symptom is observed with the module NM-HDV2-2T1/E1 with VWIC2-2MFT-T1/E1. This issue could impact other modules as well.

  Workaround: There is no workaround other than from removing SNMP.

- CSCuc59738

  Symptoms: Memory leak is seen in Chunk Manager due to a CCE DP feature.

  Conditions: This symptom occurs in ZBFW configurations with a good number of ACLs used for QoS settings.

  Workaround: Periodic reload of the router recovers the leaked memory.

- CSCuc60057

  Symptoms: When sending a fax through the Canon machine, through the MGCP BRI, the fax sends three copies instead of one. In the PCM captures taken for the failed fax on the BRI port, an MCF for a EOP is received. However, the machine keeps sending the EOP twice and then disconnects, resulting in the fax being sent thrice.

  Conditions: This symptom is observed only with the Canon 1140 machine.

Workaround: There is no workaround.

Further Problem Description: Troubleshooting was done as follows:

1. Changed the DSP firmware by using a different Cisco IOS version. Tried the latest Cisco IOS Release 15.2(2)T.
2. Tried increasing the signal strength going from the router to the machine by adjusting the gain and attenuation.
3. Tried reducing the delay between the packets by adjusting the fax play out delay.
4. Stopped any hairpinning by issuing “no local by pass”.

- CSCuc61771

  Symptoms: When upgrading CUBE Cisco IOS to Cisco IOS Release 15.2 code, the RFC2833 packets are transcoded to g.711 packets with a short DTMF duration, which are followed by transcoded RFC2833 packets. With Cisco IOS Release 15.1 code, there are no RFC2833 packets on the PCM side and the inband DTMF duration is correct.

  Conditions: This symptom occurs in PCM transcoding mode. One side has DTMF inband and the other side is RFC2833 dtmf-relay, and dtmf-relay is configured. This issue is seen with Cisco IOS Release 15.2.x and PVDM3.

  Workaround: Downgrade Cisco IOS to Cisco IOS Release 15.1M&T code or use PVDM2.

- CSCuc62051

  Symptoms: Nile manager crashes on configuring the G.8032 on the Cisco ASR 903 router.

  Conditions: This symptom is timing issue and can be seen while configuring the G.8032 configuration, along with interface configurations from bootflash. This issue is not easy to reproduce because of timings.

  Workaround: There is no workaround.

- CSCuc63884

  Symptoms: A router configured with HSRP and RF interdev may experience an NMI watchdog during reload after failover, as it transitions from a standby to an active state.

  ```
  SYS-2-INTSCHED  'sleep for' at level 6
  -Process= "RF Interdev reload process", ipl= 6, pid= 316

  NMI Watchdog timeout!!: vector 2, PC = 0x219B3C
  ```

  Conditions: This symptom is observed with HSRP and interdev configured. HSRP failover is triggered by link failure if the configuration is being saved at the same time.

  Workaround: There is no workaround.

- CSCuc66518

  Symptoms: The ISM-VPN: tlb load/fetch exception is seen on the ISM.

  Conditions: This symptom is observed with site-to-site FlexVPN traffic.

  Workaround: Use the onboard crypto or software crypto engine instead of Reventon.

- 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= 23B9EA7Cz 23BA1A44z 23BA1E24z 23B712B8z 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.

- CSCuc67203

  Symptoms: Transferring of multicast over a GRE/IPsec tunnel fails if the payload size of the multicast is greater than 14K. This issue is seen only if the source is connected to a port on the EHWIC-D-8ESG module. If the source is connected to the built-in port, then the transfer is successful.

  Setup:

```
                EHWIC-D-8ESG
                    Vlan1
Source--------Testrouter1-(C1900)---------------Testrouter2(c1900)-----------Receiver
                                                      ------IPSEC/GRE-
```

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)M1 and Cisco IOS Release 15.2(2)T1 with the EHWIC-D-8ESG module.

  Workaround:

  1. Custom applications can be programmed to limit the size of individual packets to 13K and some off-the-shelf software could have configuration options to do the same.
  2. The EHWIC switch module could be bypassed by using the external switch and a built-in router port.

- CSCuc69342

  Symptoms: About 10 minutes after CUBE boot, the router crashes with the following traceback:

```
-Traceback= 5B01805 46158ED 45F4F57 45BB19E 45BA1CF 451D6DC 4525549 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.

- CSCuc70472

  Symptoms: Compression (V.42bis, V.44) is disabled by “modemcap” for PVDM2-DM. After some time, certain modems start to negotiate V.44/V.42bis and drop those calls before PPP. The number of modems negotiating compression is growing over time, leading to an increase in the drop call rate.

  Conditions: This symptom occurs when the following modemcap is applied:

```
"modemcap entry V32bis_noComp1:MSC=&F0+DCS=0,0;+MS=10,0,4800,14400" OR
  "modemcap entry V32bis_noComp2:MSC=+MS=10,0,4800,14400;%C0"
```

  Breakdown:

```
  "+DCS=0,0=0,0" - V.44 OFF, V.42bis OFF
  "+MS=10,0,4800,14400" - V.32bis,No V8.bis, min 4800, max 14400
  "%C0" - No compression
```

  After reload:

```
Router#sh modem log 0/463 | i compression
 Data compression                69    None
 Data compression                69    None
 Data compression                69    None
 Data compression                69    None  << No compression
Router#sh modem configuration 0/463 | i S41|S82
    S41 = 137     Compression selection is MNP 5 Retrain and fallback/fall
forward disabled
    S82 = 128     Break Handling Options/LAPM Break Control = 0x80
    S82 = 21
```

  A few hours/days after reload:

```
Router#sh modem log 0/463 | i compression
 Data compression                68    None
 Data compression                68    V44 << Starts to negotiate V.44, even
while disabled by modemcap
 Data compression                68    V44
 Data compression                68    V44
Router#sh modem configuration 0/463 | i S41|S82
    S41 = 139     Compression selection is MNP 5 and V.42 bis
    S82 = 128     Break Handling Options/LAPM Break Control = 0x80
    S82 = 25
```

  Workaround: Reload.

- CSCuc70958

  Symptoms: The Cisco ISR-3825 has a latency in traffic processing and tx_ping counter on phy controllers are increasing and not getting emptied.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(24)T8.

  Workaround: Reload the router.

- CSCuc71422

  Symptoms: CUBE crashes if it fails to route an INVITE that has a Replaces: header.

  Conditions: This symptom occurs when an INVITE with a Replaces: header is received but all outbound dial peers failed to connect the call.

  Workaround: There is no workaround.

- CSCuc71493

  Symptoms: Significant transaction time degradation is observed when an e-mail with attachment(s) is sent from the Windows 7 client using Outlook to a server running Outlook 2010 on the Windows 2008 server and the WAN latency is low, that is, ~12ms RTT.

  Conditions: This symptom is observed when the client is Windows 7 and data is being uploaded using the MAPI protocol and the connection is being optimized by WAAS-Express.

  Workaround: Disable WAAS-Express.

- CSCuc71706

  Symptoms: Execution of the **show run** command and other commands such as **copy run start** and **show access-list** cause the router to stop for a few minutes before completing.

  Conditions: This symptom is observed with Cisco ISR G2 routers. This issue is seen only with IPV6 configured and used.

  Workaround: There is no workaround.

- CSCuc71885

  Symptoms: A crash is seen at cce_dp_csdb_api_retrieve_feature_object.

  Conditions: This symptom is observed with spoke-to-spoke UDP traffic, SIP, and DNS, which causes the crash on the traffic initiator.

  Workaround: There is no workaround.

- CSCuc72114

  Symptoms: Participating router ports of Etherchannel do not get suspended upon speed/duplex mismatch.

```
RMS-rtr1-st0159#sh int po1
Port-channel1 is up, line protocol is up
  Hardware is GEChannel, address is c47d.4ffd.c390 (bia c47d.4ffd.c390)
  Description: ** Store LAN Interface PORT CHANNEL 1 **
  MTU 1500 bytes, BW 110000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 255/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 2
        Member 0 : GigabitEthernet0/1 , Full-duplex, 100Mb/s
        Member 1 : GigabitEthernet0/0 , Full-duplex, 10Mb/s
```

  In conditions like this, the router keeps sending traffic on a suspended link on the switch side due to load balancing and switch drops, which causes network outage. On the switch side, interfaces go into suspended mode as expected.

  Conditions: This symptom is observed with the following conditions:

  1. Etherchannel is configured between the Cisco ISR/G2 router and a Cisco Catalyst switch.
  2. There is a speed mismatch between the participating ports.

  Workaround: There is no workaround.

- CSCuc72325

  Symptoms: A router does not recognize a UA frame after sending an SNRM frame.

  Conditions: This symptom occurs when SDLC is configured on the Cisco3845 with HWIC-4T.

  Workaround: Shut/no shut the serial interface or reload the router.

- CSCuc73005

  Symptoms: The Cisco IOS firewall stops forwarding RTP packets belonging to an established session after around 30 seconds.

  Conditions: This symptom is observed with a Cisco IOS Zone-Based Firewall, with SIP inspection. This issue is seen when RTP traffic is flowing.

  Workaround: There is no workaround.

- CSCuc73036

  Symptoms: Packets cannot be set with cos value 1 with PPP encapsulation.

  Conditions: This symptom is observed with Cisco IOS Release 15.3(0.18)T.

  Workaround: There is no workaround.

- CSCuc73902

  Symptoms: An IPsec router configured in a stateful IPsec High Availability (HA) configuration may incorrectly reset the ESP sequence number when it becomes the active router after a switchover. This will result in packets drop on the peer device due to antireplay check failure, as can be observed with the following error:

  ```
  %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=X,
  sequence number=1
  ```

  Conditions: This symptom occurs only after an HA switchover event.

  Workaround: Disable the antireplay check on the VPN end peer devices by using the **crypto ipsec security-association replay disable** command.

- CSCuc74594

  Symptoms: The router fails to boot and issues a "*** Machine Check Exception ***" error message. Attempting to break the boot process results in a "WARNING: Break key" message but does not deliver a ROMMON prompt.

  Conditions: This symptom occurs when attempting to enable all licensing on a the Cisco 3945 (datak9, securityk9, uck9, hseck9).

  Workaround: There is no workaround.

- CSCuc76130

  Symptoms: IPsec SAs are not getting deleted even after removing ACL.

  Conditions: This symptom occurs when using the IPsec feature with Cisco IOS Release 15.3(0.18)T0.1.

  Workaround: There is no workaround.

- CSCuc77704

  Symptoms: The GETVPN/GDOI Secondary Cooperative Key Server (COOP-KS) does not download the policy (that is, when the **show crypto gdoi ks policy** command is issued on the Secondary COOP-KS and the command output shows that no policy is downloaded) and Group Members (GMs) registering to the Secondary COOP-KS fail to register without any warning/error message.

  Conditions: This symptom is observed when the GETVPN/GDOI group (with COOP configured) has an IPsec profile configured with one of the following transforms in its transform-set:

  - esp-sha256-hmac
  - esp-sha384-hmac

  - esp-sha512-hmac

  Workaround: Use esp-sha-hmac as the authentication transform instead.

- CSCuc78402

  Symptoms: EO-EO and DO-DO escalation scenarios fail with CUBE after SSO.

  Conditions: This symptom is observed with HA calls.

  Workaround: There is no workaround.

- CSCuc78772

  Symptoms: CPU watchdog is observed, followed by the box crashing.

  Conditions: This symptom occurs when an IPv6 ACL entry is created with the log option. If there are more than 16 different traffic matching this ACL with a high rate, the box will run out of CPU to send to the log.

  Workaround: Remove the log option from the ACL entry or create a more specific ACL to get less than 16 different traffic matching the same ACL entry.

- CSCuc79143

  Symptoms: The cellular driver should handle the profile getting inactive and should bring down the cellular interface.

  Conditions: This symptom occurs when the profile is deactivated by the HA.

  Workaround: Doing a “clear line” will bring down the cellular interface and restore the connection.

- CSCuc79606

  Symptoms: An unexpected reboot occurs on the Cisco VG224.

  Conditions: This symptom occurs when no crashinfo file is generated. The show version indicates “System returned to ROM by power-on”.

  Workaround: This issue may not occur when running Cisco IOS Release 15.0.M.

- CSCuc80398

  Symptoms: NBAR does not match the RTP payload.

  Conditions: This symptom is observed with NBAR.

  Workaround: Configure the Access-list to match the same.

- CSCuc81117

  Symptoms: The router crashes with the **reload warm** command.

  Conditions: This symptom occurs when configuring “warm-reboot” with Cisco IOS Release 15.3(1.2)T.

  Workaround: Remove the **warm-reboot** command.

- CSCuc83104

  Symptoms: Path confirmation fails for blind transfer scenarios for both SIP Line and trunk-side scenarios.

  Conditions: This symptom is observed if “no supplementary-service sip refer” is configured.

  Workaround: Configure “supplementary-service sip refer”.

- CSCuc85321

  Symptoms: Cisco IOS may crash when AnyConnect is used.

  Conditions: This symptom is observed with the following conditions:

- The router is configured as the SSL VPN gateway.
- AnyConnect users make VPN connections to this router.

Workaround: There is no workaround.

- CSCuc89674

  Symptoms: A Cisco IOS device (UC540, ISR) running Cisco IOS Release 15.1(4)M5 experiences memory leak in the Packet Header of Chunk Manager. datagram_done is not called in some feature path which causes *Packet Header* leak, and thus “CCE dp subblock” is not freed.

  The output for the **show proc mem sorted** and **show chunk summary** commands shows the leak. The device eventually crashes due to low memory.

  Conditions: This symptom is observed with the following conditions:

  - Cisco IOS Release 15.1(4)M5.
  - QoS (service-policy), NAT, and CBAC are configured.

  Workaround: Schedule a proactive reload of the device to avoid an unexpected crash.

- CSCuc90198

  Symptoms: Cisco C892FSP-K9 is getting reloads with qos_sanity script configurations.

  Conditions: This symptom is observed with Cisco IOS Release 15.3(0.18)T0.1.

  Workaround: There is no workaround.

- CSCuc91717

  Symptoms: The router crashes when making a basic x25 configuration change.

  Conditions: This symptom occurs when the x25 translation statement is removed from the running configuration when traffic is on.

  Workaround: There is no known workaround. A possible workaround may be to shut the interface before making x25 configuration changes.

- CSCuc91949

  Symptoms: When using Cisco ISR Websecurity with Cisco Scansafe, sometimes the redirected HTTP website can fail to load, preventing access to that web page. Tracebacks on the console may accompany this behavior.

  Conditions: This symptom occurs only on a Cisco ISR-G2 router running Cisco IOS Release 15.2(4)M, when Cisco ISR Websecurity with Cisco Scansafe connector is enabled.

  Workaround: There is no workaround.

- CSCuc92167

  Symptoms: SSH use of Diffie-Hellman (DH) exchange to negotiate keying material is insecure and may lower the security of DH exchange.

  Conditions: This symptom occurs when there are known attacks against DH that takes effort of effectively halving the length of the private key. Due to SSH use of DH private values of certain lengths, if the SSH is negotiated using AES-128 and HMAC-MD5, the time needed to recover the keys is lower than expected.

  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 3.6/3.2:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:S/C:P/I:P/A:N/E:POC/RL:U/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:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCuc93361

  Symptoms: “ip” protocol is not accepted in the **ping** command

  with the IPv6 address configured.

  Conditions: This symptom occurs when a single interface is configured with an IP address, and later, the mask alone is changed.

  For example:

```
int e0/0
ip addr 10.1.1.1 255.255.255.0
no shut
```

  Later,

```
int e0/0
ip addr 10.1.1.1 255.255.0.0
```

  Workaround: Configure a different IP address and then revert to the same address with the changed mask.

  For example:

```
int e0/0
ip addr 10.1.1.1 255.255.255.0
no shut
```

  Later,

```
int e0/0
ip addr 10.1.1.2 255.255.0.0
ip addr 10.1.1.1 255.255.0.0
```

- CSCuc93763

  Symptoms: Browsing is slow on websites that are whitelisted in the Scansafe policy.

  Conditions: This symptom is observed with the following conditions:

  1. The website advertises a window scale factor (the higher the factor, more will be the impact).
  2. Whitelisting is done using the regex pattern of the website URL.
  3. “ip tcp window-size” is configured with a value greater than 65535.

  Workaround: Change the window-size on the router to less than or equal to 65535.

- CSCuc94392

  Symptoms: The router crashes from memory corruption, but the block dump is empty in the crashinfo.

```
current memory block, bp = 0xC14F4984,
memorypool type is Processor
data check, ptr = 0xC14F49B4
bp->next(0x0) not in any mempool
bp_prev(0xFFFFFFEC) not in any mempool
========= Dump bp = 0xC14F4984 ======================

C14F4884:        0        0        0        0        0        0        0        0
C14F48A4:        0        0        0        0        0        0        0        0
```

```
C14F48C4:        0        0        0        0        0        0        0        0
C14F48E4:        0        0        0        0        0        0        0        0
C14F4904:        0        0        0        0        0        0        0        0
C14F4924:        0        0        0        0        0        0        0        0
C14F4944:        0        0        0        0        0        0        0        0
C14F4964:        0        0        0        0        0        0        0        0
C14F4984:        0        0        0        0        0        0        0        0
C14F49A4:        0        0        0        0        0        0        0        0
C14F49C4:        0        0        0        0        0        0        0        0
C14F49E4:        0        0        0        0        0        0        0        0
C14F4A04:        0        0        0        0        0        0        0        0
C14F4A24:        0        0        0        0        0        0        0        0
C14F4A44:        0        0        0        0        0        0        0        0
C14F4A64:        0        0        0        0        0        0        0        0
========= Dump bp->next = 0x0 ======================

========== Dump bp->previous = 0x0 =====================

Perhaps a Watchdog Forced Crash or CPUHOG preceding.
```

Conditions: This symptom is observed when WAAS is enabled and HTTP express accelerator is configured.

Workaround: Disable either WAAS or HTTP express or both.

- 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.

- CSCuc94687

  Symptoms: SHA2 processing in software causes low throughput or high CPU.

  Conditions: This symptom is observed with the Cisco 892 with SHA2 configured and the onboard crypto engine enabled running Cisco IOS Release 15.2(4)M and later releases.

  Workaround: There is no workaround.

- CSCuc95160

  Symptoms: After receiving the CRCX message, the Cisco AS5400 does not send 200 ok to SSW. SSW sends the CRCX message to the Cisco AS5400 again.

  Between these messages, debug outputs are displayed. It seems that the call is not disconnected completely for the end point by the previous disconnect request (the DLCX is received after the CRCX message from SSW). The end point may be stuck in call_disconnecting state.

  Conditions: This symptom is observed with MGCP. This issue occurs when the Cisco AS5400 receives DLCX before sending 200 ok for the first CRCX message.

  Workaround: There is no workaround.

- CSCuc96631

  Symptoms: Incoming calls through e1 r2 stop working in Cisco IOS Release 15.2(4)M1.

  Conditions: This symptom is observed with incoming calls through e1 r2 in Cisco IOS Release 15.2(4)M1. Outgoing calls work fine.

  Workaround: Use Cisco IOS Release 15.2(2)T.

- CSCuc97106

  Symptoms: Stale/inactive sessions are seen in Cisco IOS transcoder hosted to CUBE/CME.

Conditions: This symptom is observed when the transcoder in CUBE is invoked, and if the call is escalated to T38 erroneously or intentionally, calls fail, which is normal. But, one leg remains as an inactive/stale connection, which leads to exhaustion of DSPfarm resources, eventually leading to all the calls to fail.

The call flow is as follows:

```
Sip Service provider---g711alw------CUBE---G729----------CUCM----IP phone/Fax
machine
Cube is configured for transcoder(CUBE controlled Xcoder).

CUBE01#sh sccp connections
sess_id    conn_id      stype mode     codec   sport rport ripaddr conn_id_tx

7602187     48         xcode inactive g711a   19052 2000  X.X.X.X
262209     264          xcode inactive g711a   17120 2000  X.X.X.X
```

Workaround:

- Bounce the SCCP (“no sccp”/“sccp”) or reload the router.
- If downgrading is the option, use Cisco IOS Release 15.1(2)T4 (tested in the lab).

Further Problem Description: Cisco IOS transcoder is invoked by CUBE and not hosted to CUCM, and this defect is exclusive for CUBE/CME hosted transcoders.

- CSCuc97331

  Symptoms: IPv6 EIGRP neighbors flap on a GRE tunnel.

  Conditions: This symptom occurs when tunnel protection is enabled on a IPV6 over an IPv4 tunnel.

  Workaround: There is no workaround.

- CSCuc97542

  Symptoms: The router may possibly hang during a large download via HTTP.

  Conditions: This symptom is observed Cisco IOS Release 15.x content filtering.

  Workaround: Disable Cisco IOS content filtering.

- CSCud01502

  Symptoms: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud03003

  Symptoms: A crash occurs due to “%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = CCSIP-REGISTER”.

  Conditions: This symptom occurs due to “%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = CCSIP-REGISTER”.

  Workaround: There is no workaround.

- CSCud06180

  Symptoms: When the SDK crash occurs, the cellular interface is not operational.

  Conditions: This symptom occurs when the IPSLA is present on the cellular interface, and you power-cycle the modem 8-10 times, causing the CWAN_SHIM layer to crash.

  Workaround: There is no workaround.

- CSCud06884

  Symptoms: Packets sent by CUBE have authentication failures after transfer.

  Conditions: This symptom occurs when SRTP is being used.

  Workaround: There is no workaround.

- CSCud06887

  Symptoms: IPsec Stateful failover is configured between two routers.

  router_1 is chosen as Active.

  router_2 is chosen as Standby.

  router_3 acts as the VPN end peer.

  - A VPN tunnel is created between the VIP of routers 1 and 2 and router_3.
  - SPIs are replicated from Active (router_1) to Standby (router_2).
  - After switchover from Active to Standby (done by reload of Active router_1), router_2 becomes Active and takes over the VPN connection.
  - router_1 comes up after manual reload and then reloads again by itself.
  - When router_1 comes up after the second reload, SPIs are not replicated from Active router_2.

  Conditions: This symptom occurs when IPsec Stateful failover is configured on Cisco IOS Release 15.2(4)M1. This issue is seen when the HW crypto engine is enabled.

  Workaround: There is no workaround. When next switchover from Active to Standby will be triggered, then new VPN connection is being created, packet loss occurs.

- CSCud08595

  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to multiframe established.

  Conditions: This symptom occurs 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.

- CSCud12555

  Symptoms: The number of active calls looked up through SNMP OID 1.3.6.1.4.1.9.9.63.1.3.8.1.1.2.2 is sometimes displayed incorrectly. The call count does not decrement when a call terminates. The number of active calls seems to slowly increase over a period of time and there are active call display even when there are no calls in the system.

  Conditions: This symptom is observed with Cisco 3945E routers running Cisco IOS Release 15.2(4)M1, but the exact condition is unknown.

  Workaround: There is no workaround.

- CSCud13862

  Symptoms: The Cisco WS-SUP720 running Cisco IOS Release 12.2(33)SRE3 crashes.

  Conditions: This symptom occurs during a CPU process history update.

  Workaround: There is no workaround.

- CSCud15104

  Symptoms: The Cisco VG224 loops packets on a blocking port when ports fa0/0 and fa0/1 are bridged and the blocking port resides on the Cisco VG224.

Conditions: This symptom is triggered on reload/power cycle of the Cisco VG224.

Workaround: Shut/no shut the blocking port.

- CSCud16230

  Symptoms: DTR is not detected on the Cisco HWIC-2T after disconnecting the X.21 cable.

  Conditions: This symptom is observed with the Cisco HWIC-2T.

  Workaround: There is no workaround.

- CSCud16241

  Symptoms: The serial interface does not go up immediately after starting traffic from the X.25 device.

  Conditions: This symptom is observed with the following conditions:

  - DTR is up when starting traffic from the X.25 device.
  - The Cisco HWIC-4A/S is used.

  Workaround: There is no workaround.

- CSCud16512

  Symptoms: The EIGRP route is not redistributed into BGP as the VPNv4 route with specific steps.

  Conditions: This symptom occurs during redistribution from EIGRP to BGP with VRF.

  Workaround: There is no workaround.

- CSCud16693

  Symptoms: The Cisco 3600 may crash when applying a policy-map with multiple conform actions with a table-map configuration.

```
policy-map IPVPN-10/10/50-Service-testing
class TEST-1
police cir 10000000 bc 312500
conform-action set-qos-transmit 4
conform-action set-cos-transmit dscp table dscp-cos
exceed-action drop

class TEST-2
police cir 10000000 bc 312500
conform-action set-qos-transmit 4
conform-action set-cos-transmit dscp table dscp-cos
exceed-action drop

class class-default
police cir 50000000 bc 1000000
conform-action set-cos-transmit dscp table dscp-cos
conform-action set-qos-transmit 3
exceed-action drop
```

  Conditions: This symptom is observed when applying a policy-map with multiple conform actions with a table-map configuration on the Cisco 3600.

  Workaround: Do not apply a policy-map with multiple conform actions with table-map configuration. This configuration is not supported.

- CSCud16702

  Symptoms: After a period of time (usually several days to several weeks), the Cisco AS5400 stops responding to SIP responses from the SIP server for outbound calls. There are no inbound calls from SIP. All calls are from TDM to SIP.

The call flow is as follows:

```
TDM-->DS3(7 NFAS groups of 3 PRIs each)[-->GW-->SIP]
```

Conditions: This symptom occurs when the Cisco AS5400 upgraded from Cisco IOS Release 12.4(24)T6 to Cisco IOS Release 15.1(4)M4, has been working for over a year. There is no apparent trigger for this issue. The customer needed to upgrade Cisco IOS for a new feature offered by the SIP service provider.

Workaround: Reload the gateway.

- CSCud20036

  Symptoms: The multicast operation operating over a DMVPN topology is inconsistent between Cisco routers/IOS images. The application works correctly with a Cisco 891 or 1841, but fails when using a Cisco 5915.

  This issue is seen with two of the DMVPN spoke configurations: one is a Cisco 891 and one is a Cisco 5915 ESR. Multicast traffic from each spoke is intended to be NATed into the DMVPN tunnel using different dynamic NAT address ranges at each spoke.

  The routers have identical configurations. The multicat NATed functions as expected on a Cisco 891 running the c890-universalk9-mz.150-1.M7.bin image and on a Cisco 1841 running the with c1841-advipservicesk9-mz.150-1.M2.bin image.

  The Cisco 5915 ESR appears to not be performing the Multicast NAT correctly. This symptom is that the PIM-SM Registers from the Cisco 5915 to the DMVPN Hub/RP are not using the NATed source IP address. The Cisco 5915 is running the c5915-adventerprisek9-mz.SPA.152-2.GC.bin image. When this occurs, in a joined group, the Hub never sends a register stop and PIM-SM Register packets continue indefinitely for that (S,G).

  Note that this issue is sporadic; sometimes, the Cisco 5915 sends PIM-SM Register packets which are NATed correctly. In this case, the spoke correctly receives a PIM Join and PIM Register-Stop from the Hub for that (S,G) and sends the multicast packets natively (no-longer encapsulated in PIM Register messages). However, even in this case, there is a different issue. These NATed multicasts seem to be duplicated as they are placed into the tunnel before they get encrypted.

  Working:

  ```
  Cisco 891 with c890-universalk9-mz.150-1.M7.bin (show tech-support attached)
  Cisco 1841 with c1841-advipservicesk9-mz.150-1.M2.bin (show tech-support  attached)
  ```

  Confirmed not working:

  ```
  Cisco 5915 with c5915-adventerprisek9-mz.SPA.152-2.GC.bin (show tech-support attached)
  ```

  Conditions: This symptom does not occur under any specific conditions.

  Workaround: There is no workaround.

- CSCud20092

  Symptoms: The switch crashes.

  Conditions: This symptom occurs when you apply policy-map referencing table-map to a service instance on a switch port.

  Workaround: There is no workaround. The CLI is unsupported.

- CSCud21066

  Symptoms: The Scansafe feature is not available on the c880-universalk9-voice image.

  Conditions: This symptom is observed with the c880-universalk9-voice image.

  Workaround: There is no workaround.

- CSCud22148

  Symptoms: The E1 (E&M) controller is down.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(4)M2 or later releases. This issue is seen with the Cisco 3945.

  Workaround: There is no workaround.

- CSCud25056

  Symptoms: %CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify fails for connection id=2043 local=20.2.10.2 remote=20.4.10.2 spi=B5891B95 seqno=000069CD.

  Conditions: This symptom is observed with data traffic between GMs on the same GETVPN GDOI domain, and the traffic is through the 4G/LTE interface.

  Workaround: There is no workaround.

- CSCud26401

  Symptoms: The PVDMs are marked as B, so no more users can log in after all lines are marked as B.

  Conditions: This symptom is observed after the router runs for a few days. After around two months, all lines would be marked B.

  Workaround: Reload the router.

- CSCud26633

  Symptoms: Throughput performance drop has been seen between Cisco IOS Release 15.2(2)T1.14 and Cisco IOS Release 15.2(2)T2.3.

  Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.2(2)T1.14 to Cisco IOS Release 15.2(2)T2.3.

  Workaround: There is no workaround.

- CSCud27997

  Symptoms: The router always crashes when two PVDM2-xDM are installed. If only one is installed, it works regardless of the stick or slot combination.

  Conditions: This symptom occurs on the Cisco 3900E router. The Cisco non-E 3900 router has no issue.

  Workaround: Use one PVDM or use a plain Cisco 3900 router.

- CSCud30293

  Symptoms: High CPU is seen due to the DSMP process.

  Conditions: This symptom is observed with the DSMP process.

  Workaround: There is no workaround.

- 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.

- CSCud34809

  Symptoms: The ISM module on the cisco 3900 router suddenly fails to encrypt IPsec data on specific tunnels.

Conditions: This symptom occurs when ISM-VPN-39 is installed and active on the Cisco 3900 router. This issue is seen when the Cisco 3900 router is an IPsec endpoint.

Workaround: Reloading the router is the only way to resolve this issue. Clearing IPsec SAs and/or crypto configuration will not resolve this issue.

- CSCud36086

  Symptoms: The EZVPN server may initiate negotiation to the client, even though it should not.

  Conditions: This symptom was first observed with Cisco IOS Release 15.1(1)S1 but is not exclusive to it.

  Workaround: There is no workaround.

- CSCud36723

  Symptoms: RPF information for IPv6 multicast mroutes is not updated when routing changes.

  Conditions: This symptom occurs when an IPv6 multicast configuration is present in the startup configuration.

  Workaround: After startup, remove all IPv6 multicast configurations, if any, and then apply the configuration as needed.

# Resolved Caveats—Cisco IOS Release 15.3(1)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.3(1)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsq83006

  Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.

  Conditions: This 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, and not a port-channel, this issue is not seen.

- CSCsr06399

  Symptoms: A Cisco 5400XM may reload unexpectedly.

  Conditions: This symptom is intermittent and is seen only when the DSPs available are insufficient to support the number of calls.

  Workaround: Ensure that sufficient DSPs are available for transcoding.

- CSCsy93069

  Symptoms: After a period of Telepresence calls, tracebacks and then a router crash is seen.

  Conditions: This 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.

- CSCsz05848

  Symptoms: High CPU utilization for DHCP client process.

  Conditions: This symptom is observed when 10k PDPs sessions are established.

  Workaround: There is no workaround.

- CSCtd54694

  Symptoms: A crash is seen for the **show cdp neighbor port-channel** *no and* **show cdp neighbor port-channel** *no* **de?** commands.

  Conditions: This symptom is a rare timing issue.

  Workaround: Use the **show cdp neighbor** and **show cdp neighbor detail** commands for brief and detailed CDP information. Also, the **show cdp neighbor** *interface type no* can be used with the exception that the *interface type* argument should not be *port-channel*.

- CSCth71093

  Symptoms: Routers configured to dump core to flash: or flash0: fail to dump correctly to a 4GB CompactFlash card.

  Conditions: This symptom is observed with the following configuration:

  ```
  (Cisco 3925) exception flash all flash0:
  (Cisco 3825) exception flash all flash:
  ```

  Then, when you issue a **wr core**, it fails to dump core files.

  Workaround: Dump cores to TFTP.

- 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 Cisco IOS Release 12.4(15)T14.

  Workaround: Remove CEF.

- CSCtk15666

  Symptoms: The Cisco IOS password length is limited to 25 characters.

  Conditions: This symptom is observed on Cisco NG3K products.

  Workaround: There is no workaround.

  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:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtn15610

  Symptoms: Cisco IOS may crash with a bus error accessing addr=0x0 after DSP reset.

Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T13a engineering special.

Workaround: There is no workaround at this time.

- CSCto32884

  Symptoms: The IPsec session does not come up.

  Conditions: This symptom occurs if the ISM VPN Accelerator is used and dual ACLs are configured with IP inspect turned on.

  Workaround: The only possible workaround is to disable IP inspect while this issue is resolved.

- CSCto87436

  Symptoms: In certain conditions, IOS device can crash, with the following error message printed on the console:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Proc
  ```

  Conditions: In certain conditions, if an SSH connection to the IOS device is slow or idle, it may cause a box to crash with the error message printed on the console.

  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 6.3/5.5: 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:H/RL:OF/RC:C

  CVE ID CVE-2012-5014 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

- CSCto88178

  Symptoms: Packet corruption is observed when NAT processes an H.323 packet that has some trailing data beyond the User-User Information Element.

  Conditions: This symptom occurs when NAT is configured to process H.323 packets, and it encounters an H.323 packet that has some trailing data beyond the User-User Information Element.

  Workaround: Although it is not feasible for most implementations, using the **no ip nat service H225** command prevents the packet corruption. Additionally, this issue is not present in those releases that have NAT TCP ALG support enabled.

- CSCtq17444

  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 a voice gateway for H.323.

  Workaround: There is no workaround.

- CSCtq41512

  Symptoms: After reload, ISDN layer 1 shows as deactivated. Shut/no shut brings the PRI layer 1 to Active and layer 2 to Multi-frame established.

  Conditions: This symptom occurs 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.

- 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 issue will only occur when there is a large amount of fragmentation occurring. This issue has only been seen when “ip mtu 1500” is 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.

  Workarounds 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.

- CSCtr45287

  Symptoms: 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.

- CSCts08224

  Symptoms: Expected ACL/sessions not found for most of the protocols.

  Conditions: This symptom is observed with expected ACL/sessions.

  Workaround: There is no workaround.

- CSCts54641

  Symptoms: Various small, medium, or big VB chunk leaks are seen when polling EIGRP MIB or during SSO.

  Conditions: This symptom is observed when MIBs are being polled or SSO is done.

  Workaround: There is no workaround.

- 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 2 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 a Cisco IOS XE Release 3.4S or 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 rel9 or above and the other SAF forwarder is running EIGRP SAF rel8 or below.

  Workaround: Make sure each SAF forwarder is running EIGRP rel8 or below, or rel9 or above.

- CSCts87612

  Symptoms: Traffic over L2TPv3 becomes very slow. Ping shows high latency.

  Conditions: This symptom is observed when EHWIC-1GE-SFP-CU is used as the xconnect interface.

  Workaround: Do shut/no shut on the EHWIC-1GE-SFP-CU interface

- CSCtt40285

  Symptoms: The router crashes. The following message is displayed:

  ```
  System returned to ROM by bus error at PC 0x629D2EBC, address 0xB0D0B11 at
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x629D2EBC
  ```

  Conditions: This symptom is observed across multiple Cisco IOS Releases such as Cisco IOS Release 15.1(4)M2 and Cisco IOS Release 15.2(4)M1. This issue occurs only if NAT SIP ALG processing is enabled on the router.

  Workaround: This crash can be prevented by disabling NAT SIP ALG processing on the router by issuing the **no ip nat service sip** command.

- CSCtt42330

  Symptoms: Alignment correction or a crash is seen at dx_mrvl_fdb_next and eswge_mactable_walk.

  Conditions: This symptom occurs when the **show mac-address-table** command is issued, and simultaneously there is a change in the table entries.

  Workaround: There is no workaround.

- CSCtu07968

  Symptoms: A Cisco 890 router may provide incorrect performance monitor statistics and omit some incoming packets from being handled by flexible netflow.

  Conditions: This symptom is observed when performance monitoring or flexible netflow is enabled with IPsec over a tunnel on an input interface.

  Workaround: There is no workaround.

- CSCtu16862

  Symptoms: L4F tracebacks are observed with SMB stress test traffic. You may experience a couple of retransmissions due to that and some small performance degradation.

  Conditions: This symptom is observed with stress testing.

  Workaround: There is no workaround.

- CSCtu28696

  Symptoms: A Cisco ASR 1000 crashes with **clear ip route ***.

  Conditions: This 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.

- CSCtu54300

  Symptoms: The router crashes when you try to unconfigure the crypto.

  Conditions: This symptom is observed when you clear the crypto and VRF configuration using automated scripts. The crash is seen after the test is repeated three or four times. Before the crash, the VRF and crypto features/functions are working fine.

  Workaround: There is no workaround.

- CSCtw41214

  Symptoms: ACEs are not source IP translated in multidomain authentication (MDA) mode.

  Conditions: This symptom is observed in MDA mode.

  Workaround: There is no workaround.

- CSCtw45480

  Symptoms: Inbound GRE encapsulated traffic is dropped with the “Unknown-l4 sessions drop log” message on the router with ZBFW.

  Conditions: This symptom is observed when router self-zone policies are applied and the GRE tunnel is in an intermediate zone between the inside and outside zones.

  Workaround: Remove the self-zone policies.

- CSCtw52819

  Symptoms: OQD drops on the mGRE tunnel.

  Conditions: This symptom is observed with an mGRE tunnel.

  Workaround: There is no workaround.

- CSCtw76527

  Symptoms: The crypto session stays in UP-NO-IKE state.

  Conditions: This symptom occurs when using EzVPN.

  Workaround: There is no workaround.

- 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 ASR 1000 series router, this configuration causes the creation of full VAIs 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.

- CSCtx06813

  Symptoms: Installation fails, “rwid type l2ckt” error messages appear, and the VC may fail to come up on Quad-Sup router only. Though this error may appear for multiple other reasons, this bug is specific to Cisco Catalyst 6000 Quad-Sup SSO only.

  Conditions: This symptom is observed in a scaled scenario, doing second switchover on Quad-Sup router.

  Workaround: There is no workaround.

- CSCtx15799

  Symptoms: An MTP on a Cisco ASR router sends an “ORC ACK” message through CRC for the channel ID that is just received but does not reply to the ORC for the next channel.

Conditions: This symptom is observed when there is a very short time lapse between the ORC and CRC, say 1 msec.

Workaround: There is no workaround.

- CSCtx34823

  Symptoms: OSPF keeps on bringing up the dialer interface after idle-timeout expiry.

  Conditions: This symptom occurs when OSPF on-demand is configured under the dialer interface.

  Workaround: There is no workaround.

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCtx39953

  Symptoms: KRON policy is causing a system crash.

  Conditions: This symptom is observed when using a Cisco 1921/K9 with Cisco IOS Release 15.2(T) and using KRON to schedule telnet sessions in order to check the state of VPN connections. Below is a configuration sample:

```
kron occurrence START-VPN in 1 recurring
 policy-list START-VPN
!
kron policy-list START-VPN
 cli telnet xx.xx.xx.xx 12 /source-interface GigabitEthernet 0/1 /quiet
 cli telnet yy..yy.yy.yy 42 /source-interface GigabitEthernet 0/1 /quiet
 cli telnet zz.zz.zz.zz. /source-interface GigabitEthernet 0/1 /quiet
where xx yy and zz are ip addresses of the remote hosts
```

  Workaround: There is no workaround.

- CSCtx42223

  Symptoms: The connection with an FRR client that is registered for a BFD session is lost after an SSO. FRR cut-cover time is much more than 50ms, which is not expected.

  Conditions: This symptom is observed after an SSO, when the FRR client is registered for a BFD session.

  Workaround: Bring down the BFD session and configure it again.

- CSCtx48753

  Symptoms: Higher memory usage with PPP sessions than seen in Cisco IOS XE Release 3.4S/3.5S.

  Conditions: This symptom is observed with configurations with PPP sessions. These will see up to 10 percentage higher IOS memory usage than in previous images.

  Workaround: There is no workaround.

- CSCtx54882

  Symptoms: A Cisco router may crash due to a 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.

- 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.

- CSCtx67028

  Symptoms: Tracebacks are seen during a traffic condition when DMVPN and WAAS-Express are configured.

  Conditions: This symptom is observed while initiating an FTP session from the GW, where GW DMVPN and WAAS-Express are configured.

  Workaround: There is no workaround.

- CSCtx74051

  Symptoms: When doing an ISSU downgrade, IPv6 flexible netflow monitors may be displayed and the running configuration is shown with incorrect sub-traffic types.

  Conditions: This symptom occurs upon a downgrade to Cisco IOS Release 15.2(1)S (Cisco IOS XE Release 3.5S). The monitors affected are those applied to IPv6. For example, CLI such as:

  **interface fa0/0/0**

  **ipv6 flow monitor monitor-name input**

  Workaround: Netflow code should still capture packets as expected on Cisco IOS Release 15.2(1)S. However, a reboot of the device should be done before saving the running configuration as the affected configuration saved will be incorrect and so will then fail to work on startup.

- CSCtx75190

  Symptoms: In a multihomed setup, set up the traffic as explained in the DDTS. Once end-to-end traffic flows fine, do a RP switchover on ED1. Traffic from Ixia 3 to Ixia 1 and Ixia 3 to Ixia 2 on odd VLANs (ED1 is the AED for odd VLANs) is dropped with UnconfiguredMplsFia counters incrementing.

  Conditions: This symptom is observed when you do an RP switchover with a scaled OTV configuration in a multihomed setup.

  Workaround: There is no workaround.

- CSCtx80535

  Symptoms: DHCP pool that is configured for ODAP assigns the same IP to multiple sessions.

  Conditions: This symptom is observed when PPP users receive pool via Radius. The pool is defined on the Cisco 10000 series router to use ODAP. ODAP is receiving the subnets from Radius correctly, and assigns IPs to PPP sessions, but sometimes two users end up having the same IP address.

  Workaround: Clear both sessions sharing the same IP.

- CSCtx82538

  Symptoms: This DDTS has been raised to remove platform-specific macros.

  Conditions: This symptom is observed with CPU-specific checks. CPU-specific checks should not be in PI code. Use of shims are required.

  Workaround: Remove the CPU-specific check.

- CSCtx85623

  Symptoms: The ATM output queue is stuck, and the dialer loses the IP address. The following error messages are displayed:

```
Jul  5 10:16:45.430: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
Jul  5 10:16:45.442: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
Jul  5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access2, changed state to down
Jul  5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2,
changed state to down
Jul  5 10:16:46.430: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1,
changed state to down

Dialer Interface loses IP Address
n0920ar101#sh ip int brief
Interface                  IP-Address      OK? Method Status
Protocol
Dialer1                    unassigned      YES IPCP   up                    up

Output Queue is Stuck at 40/40 and Drops increment at the VC Level
n0920ar101#sh queueing int atm0/3/0
Interface ATM0/3/0 VC 8/35
Queueing strategy: fifo
Output queue 40/40, 830 drops per VC << reaches 40/40 and drops increment at
the VC level

sn0920ar101#sh queueing int atm0/3/0
Interface ATM0/3/0 VC 8/35
Queueing strategy: fifo
Output queue 40/40, 833 drops per VC << reaches 40/40 and drops increment drops
increment at the VC level
```

  Conditions: This symptom is observed with a Cisco ISR G1/G2 with HWIC-1ADSL Card, SRE/WAE. Crypto is enabled under the dialer interface, and CEF is also enabled. All these conditions are be necessary to trigger the symptom.

  Workaround 1: Reconfigure PVC(PVC reset will work only 23 times, after which reload is required).

  Workaround 2: Disable the hardware crypto engine accelerator.

  Workaround 3: Disable CEF.

  Workaround 4: Reload the router.

- 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 symptom is observed 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.

- CSCty03133

  Symptoms: Memory leak in IPsec key engine process.

  Conditions: This symptom is observed with the following conditions:

  - Scale 1000 IKE * 1 Vrf * 4 IPSec, total 4K IPSec sessions.
  - Multi-SA enabled.
  - CAC=50,DPD=60 periodic.
  - ~10M bidirectional traffic.

  Workaround: There is no workaround.

- CSCty12524

  Symptoms: A BRI packet from LMA is not handled properly on MAG and MAG is not sending the APN and SSMO option in PBRA.

  Conditions: This symptom is observed on the originating or old MAG while clearing sessions in LMA in response to mobile node roaming to a new MAG.

  Workaround: There is no workaround.

- CSCty16106

  Symptoms: IKE/GDOI bypass policy entries (four entries) are downloaded to PAL dataplane SADB as part of the initial policy download. But, as IKE/GDOI traffic is never routed to tunnel interfaces, the entries are not required for tunnel protection cases.

  Conditions: This symptom is observed with IKE/GDOI bypass policy entries.

  Workaround: There is no workaround.

- CSCty17288

  Symptoms: MIB walk returns looping OID.

  Conditions: This symptom is observed when a media mon policy is configured.

  Workaround: Walk around CiscoMgmt.9999.

- 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.

- CSCty27687

  Symptoms: A core dump generated by a Cisco 3900/3900e with 2GB or more shows up as being corrupt in GDB. This prevents the core dump from being used to do a more detailed analysis of a crash.

  Conditions: This symptom is observed with a core dump generated on a Cisco 3900 or Cisco 3900e with more than 2GBs. Cores generated with 1GB of memory can be loaded into informers.

  Workaround: There is no workaround.

- CSCty35726

  Symptoms: The following error message is displayed on the logs:

  ```
  InterOp:Cube-NavTel : LTI: Video Xcode Call with plain Audio FAILS
  ```

  Conditions: This symptom is seen when video Xcode call with plain audio fails.

  Workaround: There is no workaround.

- 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 releases.

  Workaround 1: Add the following commands to change the TCP segmentation on the router:

  ```
  router(config)# ip tcp mss 1400
  router(config)# ip tcp path-mtu-discovery
  ```

  Workaround 2: Use a different validation method (CRL) when possible.

- CSCty57856

  Symptoms: The Standby router crashes for an SRTP call on Active.

  Conditions: This symptom occurs intermittently. This issue is seen due to a transient scenario, where unstable data from Active is checkpointed on Standby.

  Workaround: There is no workaround.

- CSCty61216

  Symptoms: CCSIP_SPI_Control causes a leak with a Cisco AS5350.

  Conditions: This symptom is observed with the following IOS image: c5350-jk9su2_ivs-mz.151-4.M2.bin.

  This issue is seen with an outgoing SIP call from gateway (ISDN PRI --> AS5350 --> SIP --> Provider SIP gateway).

  Workaround: There is no workaround.

- CSCty64255

  Symptoms: BGP L3VPN dynamic route leaking feature from the VRF to global export feature, the prefix-limit is incorrect upon soft clear, or new prefix added, or prefix deleted.

  Conditions: This symptom is observed when VRF to global export is enabled, and prefix-limit is configured.

  Workaround: BGP hard clear.

- CSCty65189

  Symptoms: Incoming register packets are dropped at the RP when the Zone-Based Firewall (ZBFW) is configured on the RP.

  Conditions: This symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- 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.

- CSCty71843

  Symptoms: Tracebacks are observed at lfd_sm_start and lfd_sm_handle_event_state_stopped APIs during router bootup.

  Conditions: This symptom is observed with L2VPN (Xconnect with MPLS encapsulation) functionality on a Cisco 1941 router (acting as edge) running Cisco IOS interim Release 15.2(3.3)T. This issue is observed when a router is reloaded with the L2VPN configurations.

  Workaround: There is no workaround.

- CSCty74859

  Symptoms: Memory leaks on the active RP and while the standby RP is coming up.

  Conditions: This symptom is observed when ISG sessions are coming up on an HA setup.

  Workaround: There is no workaround.

- CSCty80553

  Symptoms: The 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 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.

- CSCty89224

  Symptoms: A Cisco IOS router may crash under certain circumstances when receiving a MVPNv6 update.

  Conditions: This symptom occurs when an MVPNv6 update is received.

  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 6.8/5.6:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-3895 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

- CSCty90223

  Symptoms: A crash occurs at nhrp_nhs_recovery_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. 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.

- CSCtz02622

  Symptoms: FlexVPN spoke crashed while passing spoke-to-spoke traffic.

  Conditions: This symptom is observed during passing of traffic from spoke-to-spoke or when clearing IKE SA on the spoke.

  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 6.1/5:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-3893 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

- CSCtz03779

  Symptoms: The standby RSP crashes during ISSU.

  Conditions: This symptom occurs when you perform an ISSU downgrade from Cisco IOS XE Release 3.6S to Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCtz08388

  Symptoms: The 86x VAE platform DSL line cannot train up with the ADSL2/ADSL2+ profile after you manually shut/no shut the DSLAM port.

  Conditions: This symptom is observed with the following conditions:

  1. Connect 86x VAE DSL WAN port to DSLAM port (either ADSL2/ADSL2+ profile).
  2. Disable/enable the port and the line will not train up again.

  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.

- CSCtz15274

  Symptoms: When attempting a T.38 fax call on gateway, you may see the following in the logs:

  ```
  006902: %FLEXDSPRM-3-UNSUPPORTED_CODEC: codec cisco is not supported on dsp 0/0
  006903: %FLEXDSPRM-5-OUT_OF_RESOURCES: No dsps found either locally or globally.
  ```

  Conditions: This symptom is observed with a T.38 fax call.

  Workaround: There is no workaround.

- CSCtz21456

  Symptoms: A router has an unexpected reload due to CCSIP_SPI_CONTROL process.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz25953

  Symptoms: The “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

  Conditions: This 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.

- CSCtz26683

  Symptoms: An unsupported “ip verify unicast ...” configuration applied to an interface may still be shown in **show running-config** after being rejected. Output similar to the following will appear when applying the configuration:

  ```
  % ip verify configuration not supported on interface Tu100
    - verification not supported by hardware
  % ip verify configuration not supported on interface Tu100
    - verification not supported by hardware
  %Restoring the original configuration failed on Tunnel100 - Interface Support
  Failure
  ```

  Conditions: This symptom occurs when there is no prior “ip verify unicast ...” configuration on the interface and when the interface and/or platform do not support the given RPF configuration.

  Workaround: In some cases, it may be possible to get back to the previous configuration by using a **no** form of the command. In other cases, it will be necessary to reload the device without saving the configuration, or editing the configuration manually if already saved.

- CSCtz26735

  Symptoms: The SDP process to provision CVO router is broken in Cisco IOS Release 15.2(3)T.

  Conditions: This symptom is seen when you start the SDP process. The connection immediately breaks after the username and password are entered.

  Workaround: There is no workaround.

- CSCtz34228

  Symptoms: When NTLM (passive/active) is configured on a Cisco ISR, the user authentication process can generate authentication failure messages.

  Conditions: This symptom is observed when user authentication sees multiple GETs from the browser.

  Workaround: Increase the max-login attempts from a default of five to a larger number.

- 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.

- CSCtz40460

  Symptoms: A router running Cisco IOS may crash or hang.

  Conditions: This symptom may be observed when SSLVPN is configured with NTLM authentication. NTLM authentication is configured by default.

  Workaround: There is no workaround.

- CSCtz40621

  Symptoms: Router crash is observed.

  Conditions: This symptom is observed when GetVPN GM tries to register to keyserver and keyserver issues a rekey simultaneously.

  Workaround: There is no workaround.

- CSCtz41048

  Symptoms: The **trace mpls ipv4** command is unsuccessful.

  Conditions: This symptom is observed with the **trace mpls ipv4** command.

  Workaround: There is no workaround.

- 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.

- 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 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.

- CSCtz47309

  Symptoms: When using smart defaults in FlexVPN, the mode transport may be sent from initiator even if “tunnel” is configured.

  Conditions: This symptom was first observed 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: This symptom is observed 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 2 seconds, three commas is 3 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, that is, 919195551212x22.

  Dialing directly to a number with no extension or extra digits works as expected.

  Workaround: There is no workaround.

- CSCtz47873

  Symptoms: The command **show crypto ikev2 client flex** does not work as expected.

  Conditions: This symptom is observed with a client/server flexVPN setup.

  Workaround: Execute either **show crypto IKEv2 sa** or **show crypto session detail**.

- CSCtz48338

  Symptoms: A router may crash with setup with configuration of BGP L3VPN VRF to global export, NSR, and large scale, hard clear or link flap.

  Conditions: This symptom is seen under the following conditions:

  1. BGP L3VPN VRF to global import.
  2. NSR.
  3. Large scale.

  Workaround: There is no workaround.

- CSCtz49200

  Symptoms: OSPF IPv6 control packets are not encrypted/decrypted.

  Conditions: This symptom is observed while configuring the IPv6 OSPF authentication.

  Workaround: There is no workaround.

- CSCtz50204

  Symptoms: A crash is observed on EzVPN Server if VRF configuration under the ISAKMP profile is modified.

  Conditions: This symptom is observed only if there are active sessions at the time of configuration change.

  Workaround: Prior to applying a configuration change, clear the sessions.

- CSCtz50683

  Symptoms: Upon removing 10 x MDLP sessions, one or more hardware adj remains. This issue occurs due to incorrect removal of LSPs.

  Conditions: This symptom is observed when more than eight sub-LSPs occur.

  Workaround: Use no more than eight sub-LSPs.

- CSCtz51773

  Symptoms: High CPU is 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: This 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**.

- CSCtz52843

  Symptoms: The following messages are displayed whenever the ATM link goes down.(Cu is deploying ADSL.)

```
Nov  2 05:27:49 EDT: %SYS-2-BADSHARE: Bad refcount in pak_enqueue,
ptr=6431A7E8, count=0,
-Traceback= 0x60BA4218 0x6035E098 0x6035FEC4 0x6064CD48 0x603676F0 0x608BABC8
0x6065D344 0x60666798
0x602D6240 0x600BA8CC 0x621D75E4 0x6004A188


Nov  2 05:27:49 EDT: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=6431A7E8, count=0,
-Traceback= 0x60BA4218 0x6035937C 0x603600C4 0x6064CD48 0x603676F0 0x608BABC8
0x6065D344 0x60666798
0x602D6240 0x600BA8CC 0x621D75E4 0x6004A188

Nov  4 08:29:27 EST: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to up

Nov  4 08:29:27 EST: %SYS-4-CHUNKMALLOCFAIL: Could not allocate chunks for ATM0/1/0

Total free: 0, Total inuse: 16, Cause : Not a dynamic chunk
 -Process= "ATM Periodic", ipl= 4, pid= 65,  -Traceback= 0x60BA4218 0x6027CB94
0x6027CBF8 0x603837A0
```

```
0x6027F688
```

Conditions: This symptom occurs when OAM is used to manage the PVC and the peer interface is down.

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.

- CSCtz63438

  Symptoms: In a GETVPN environment, the group member continuously registers to keyserver.

  Conditions: This symptom is observed when the onboard crypto engine is disabled on a Cisco 1900 series platform.

  Workaround: There is no workaround.

- CSCtz67272

  Symptoms: A crash is seen with the following error message:

```
%SCHED-0-ISRWATCHDOG: Interrupt of level 0 running for a long time
```

  Conditions: This symptom is observed with a Cisco 3945 router or any other Cisco ISR-G2 router.

  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.

- 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.

- CSCtz72044

  Symptoms: 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.

- 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.

- 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**.

- CSCtz73836

  Symptoms: The router crashes.

  Conditions: This symptom is observed when the router is running NHRP.

  Workaround: There is no workaround.

- CSCtz74685

  Symptoms: A router crash is observed on Y1731 DM.

  Conditions: This symptom is seen when starting 1DM session.

  Workaround: There is no workaround.

- CSCtz75071

  Symptoms: CSCty98523 is not fully published in Cisco IOS Release 15.2M&T.

  Conditions: This symptom is observed with CSCty98523. CSCty98523 has changes in the “crypto” and “crypto_engine” components. However, only the “crypto” changes got published in the Cisco IOS Release 15.2M&T code branch. It was causing issues for IKEv2 crypto engine operations. This DDTS was raised to publish the “crypto_engine” change part of CSCty98523 in the Cisco IOS Release 15.2M&T code branch.

  Workaround: There is no workaround.

- CSCtz76287

  Symptoms: Sometimes, the spanning tree protocol does not work properly and causes a loop in the network.

  Conditions: This symptom occurs when the router with the highest bridge ID has WLAN in the same switch and generates RBCP packets.

  Workaround: Change the bridge ID manually.

- CSCtz76650

  Symptoms: In phase 2 IPv6 DMVPN deployment, traffic for IPv6 hosts behind spokes goes via the hub.

  Conditions: This symptom is observed in IPv6 DMVPN network when using phase 2 configuration and routing protocols with link-local nexthop.

  Workaround: Do not use link-local nexthop routing, instead use unicast next-hops (for example, BGP as the routing protocol).

- 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.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6S or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

Conditions: This 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.

- CSCtz78943

  Symptoms: A Cisco router experiences a spurious access or a crash. Cisco ISR-G1 routers such as a 1800/2800/3800 experience a spurious access. ISR-G2 routers such as the Cisco 2900/3900 routers that use a Power PC processor crash because they do not handle spurious accesses.

  Conditions: This symptom occurs after enabling a crypto map on an HSRP-enabled interface. The exact conditions are being investigated.

  Workaround: There is no workaround.

  Further Problem Description: The CSCtx90408 DDTS was originally filed to fix this issue. Unfortunately, this caused another issue, which was addressed by backing out of the changes. The fix was backed out in the CSCty83376 DDTS, so this DDTS (CSCtz78943) will address both issues.

- CSCtz79991

  Symptoms: The router crashes @lic_install_notify_and_print_output.

  Conditions: This symptom is observed when license files are copied to flash of the router. After checking for EULA, the router crashes.

  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.

- CSCtz86747

  Symptoms: The router crashes upon removing all the class-maps from the policy-map.

  Conditions: This symptom is observed when a route crashes while removing all user-defined class-maps with live traffic.

  Workaround: Shut the interface first before removing the class-map.

- 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.

- CSCtz88595

  Symptoms: The NTLM VIP pop-up shows the actual server URL instead of the VIP address.

  Conditions: This symptom is observed with the NTLM authentication method and when virtual IP is configured. If GET request comes for the session already in INIT state, this issue will occur.

  Workaround: There is no workaround.

- CSCtz89334

  Symptoms: A traffic blackhole is seen while a single pair of 4-wire EFM bond connections is down on a Cisco 888E router.

  Conditions: This symptom occurs when connecting to an Ericsson DSLAM from a Cisco 888E router.

  Workaround: There is no workaround.

- CSCtz94902

  Symptoms: Memory allocation failure occurs when attaching to SIP-40 using a web browser.

  Conditions: This symptom occurs on the line card.

  Workaround: Reset the line card.

- CSCtz96167

  Symptoms: QoS DSCP cases fail.

  Conditions: This symptom is observed with a QoS profile (with DSCP as 31 configured under SBE) is being hit but DSCP bit is still sent as 0.

  Workaround: There is no workaround.

- CSCtz98486

  Symptoms: The Flexwan QoS Offered Rate is not updated.

  Conditions: This symptom occurs when traffic is flowing properly in both pos interfaces, where the offered on the policy-map o/p is not updated.

  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.

- CSCua01641

  Symptoms: The router's NAS-IP address contained in the RADIUS accounting-on packet is 0.0.0.0:

```
RADIUS:  Acct-Session-Id     [44]  10  "00000001"
RADIUS:  Acct-Status-Type    [40]  6   Accounting-On
        [7]
RADIUS:  NAS-IP-Address      [4]   6   0.0.0.0

 RADIUS:  Acct-Delay-Time     [41]  6   0
```

  Conditions: This symptom occurs when you restart the router.

  Workaround: There is no workaround.

- CSCua04049

  Symptoms: If a capture is stopped because of the limits reached and the capture is started immediately, the capture fails to stop.

  Conditions: This symptom occurs after immediate activation of a capture.

  Workaround: Clear buffer before activating the capture or wait for a minimum of 5 seconds before reactivation of a capture point.

- CSCua06476

  Symptoms: When “clear crypto sa vrf” is executed to clear a non-GETVPN SA, there is an attempt to reregister the GETVPN group members irrespective of their data plane VRF.

  Conditions: This symptom occurs when “clear crypto sa vrf” is executed to clear a non-GETVPN SA, and there is an attempt to reregister the GETVPN group members irrespective of their data plane VRF.

  Workaround: There is no workaround.

- CSCua06598

  Symptoms: The router may crash with a 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.

- CSCua06629

  Symptoms: The **sh ipv6 mobile pmipv6 mag globals** command does not show any output.

  Conditions: This symptom is observed only when domain and MAG configurations are present.

  Workaround: If MAG configuration is complete (all requisite access interfaces and peers are configured), then this issue will not be seen.

- 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 apparent after 3-4 weeks and occurs when the process is CCSIP_SPI_CONTRO.

  Workaround: There is no workaround.

- CSCua10556

  Symptoms: A few IKEv2 SAs get stuck in delete state.

  Conditions: This symptom is observed when bringing up 2k flex sessions.

  Workaround: There is no workaround.

- CSCua12945

  Symptoms: Applying QoS under the serial interface is causing the interface to flap and most of the time causes line protocol to be DOWN.

  Conditions: This symptom occurs during both congestion and noncongestion on the link.

  Workaround: Doing a shut/no shut on the interface makes the interface come UP and running.

- CSCua15003

  Symptoms: When a call is canceled midcall, the CUBE may not release the transcoder resource for the call. As a result, there is a DSP resource leak.

  Conditions: This symptom is observed with the following conditions:

  - CUBE receives 180 ringing with SDP session.
  - “media transcoder high-density” is enabled.

  Workaround: Disable “media transcoder high-density”.

- 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.
  - The 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.

- CSCua16561

  Symptoms: Jumbo-frame packets sent over IPsec VPN from a Cisco 800 series router are dropped on the receiving VPN peer.

  Conditions: This symptom is observed when the packet size is above the standard FastEthernet MTU size (the problem was observed for any packet more than 1512 bytes), and the path MTU is such that no fragmentation is needed.

  Workaround: Disable the onboard crypto accelerator:

```
no crypto engine onboard 0
```

- CSCua17746

  Symptoms: IKEv2 with RSA-Sig as auth session will fail.

  Conditions: This symptom is observed with IKEv2 + RSA-Sig auth + ISM VPN or - IKEv2 + RSA-Sig auth + 7200 with VSA.

  Workaround: Disable ISM VPN or VSA or do not use IKEv2 RSA-Sig as auth.

- CSCua18138

  Symptoms: If you enable the mobile IP function, a Cisco 819 will crash after a cable is removed.

  Conditions: This symptom is observed when redundancy group is configured under “ip mobile router”.

  Workaround: There is no workaround.

- CSCua18166

  Symptoms: When subappid 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.

- CSCua19207

  Symptoms: A Cisco ASR 1000 is unable to support class-default shaping on subinterface used with tunnel QoS from the Cisco IOS XE Release 3.1S.

  Conditions: This symptom occurs on a Cisco ASR 1000 when trying to configure class-default shaping on a subinterface used with tunnel QoS.

  Workaround: There is no workaround.

- CSCua19425

  Symptoms: RP crashes at the far end, pointing to Watchdog Process BGP.

  Conditions: This symptom is observed when doing an FP reload at the near end. This issue is seen with EBGP sessions with BFD configured between near end and far end routers.

  Workaround: There is no workaround.

- CSCua21049

  Symptoms: The recursive IPv6 route is not installed in the multicast RPF table.

  Conditions: This symptom occurs in the multicast RPF table.

  Workaround: There is no workaround.

- CSCua21166

  Symptoms: Unable to form IPsec tunnels due to the “RM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality with securityk9 technology package license.” error.

  Conditions: This symptom is observed 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: 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: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCua21201

  Symptoms: RP2 reloads unexpectedly.

  Conditions: This symptom is observed with one dynamic crypto map with 8k tunnels running 700Mbps 64B packets overnight.

  Workaround: There is no workaround.

- CSCua21238

  Symptoms: Cisco IOSd crashes at ipv6_address_set_tentative.

  Conditions: This symptom occurs while unconfiguring IPv6 subinterfaces during the loading phase of a box with Netflow configuration.

  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.

- CSCua23217

  Symptoms: Ping failure is observed.

  Conditions: This symptom is observed with DSL group pairs configured on controllers.

  Workaround: There is no workaround.

- CSCua24676

  Symptoms: The VRF to the global packet's length is corrupted by -1.

  Conditions: This symptom occurs when the next-hop in the VRF is global and recursive going out labeled. This issue is seen from Cisco IOS Release 15.0(1)S3a onwards, but is not seen in Cisco IOS Release 15.0(1)S2.

  Workaround: Use the next-hop interface IP instead of the recursive next-hop.

- CSCua24689

  Symptoms: Fragments are sent without label resulting in packet drops on the other side.

  Conditions: This symptom is observed with the following conditions:

  - MPLS enabled DMVPN tunnel on egress.
  - VFR on ingress.

  Workaround: Disable VFR if possible.

- CSCua27852

  Symptoms: Traffic loss is seen in pure BGP NSR peering environment.

  Conditions: This symptom is seen on a Cisco router that is running Cisco IOS Release 15.2(2)S, and the BGP peerings to CEs and RR are all NSR enabled.

  Workaround: Enable the **bgp graceful-restart** command for RR peering.

- CSCua28346

  Symptoms: A router crashes during second rekey.

  Conditions: This symptom occurs with IKEv2 with RSA authentication.

  Workaround: There is no workaround.

- 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.

- CSCua29428

  Symptoms: When you try to configure **router rip**, the "version" subcommand does not exist.

  Conditions: This symptom is observed with the **router rip** command.

  Workaround: There is no workaround.

- CSCua30053

  Symptoms: Authentication is failing for clients after some time because the radius_send_pkt fails, because it complains about the low IOMEM condition.

  Conditions: This symptom is observed in AAA, where the minimum IO memory must be 512KB to process the new request. If the memory is less than this, AAA does not process the new authentication request. This is an AAA application threshold. This application barriers are not valid in dynamic memory case. Such conditions are removed for the NG3K platform.

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: This symptom is observed with Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- CSCua31934

  Symptoms: Crash seen at __be_address_is_unspecified.

  Conditions: This symptom is observed with the following conditions:

  1. It occurs one out of three times and it is a timing issue.
  2. DMVPN tunnel setup between Cisco 2901 as spoke and Cisco ASR 1000 as hub.
  3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  4. It can occur with v6 traffic alone.
  5. If you remove the tunnel interface on the ASR and add it again using **conf replace nvram:startup-config** the crash will occur.

  Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua32379

  Symptoms: Cisco ASR 1000 hubs crash at crypto_ss_set_ipsec_parameters.

  Conditions: This symptom is observed with dual-hubs switchover between active-standby and active-active.

  Workaround: There is no workaround.

- CSCua33527

  Symptoms: Traceback is seen after second or third switchover:

  ```
  %LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING
  -Traceback= 7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
  ```

  Conditions: This symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.

  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.

- CSCua35884

  Symptoms: The **ipv6 cef** option is missing from serial and ATM interface commands.

  Conditions: This symptom is observed with the following CLI:

  **conf t int s0/2/0 ipv6 c**?

  ```
  Returns
  ```

Workaround: There is no workaround.

- CSCua37898

  Symptoms: Memory leaks are observed with @crypto_ss_enable_ipsec_profile on VSS.

  Conditions: This symptom is observed when OSPFv3 authentication is enabled over virtual link, and the OSPFv3 process is restarted.

  Workaround: There is no workaround.

- CSCua38881

  Symptoms: The router reloads at clear_dspm_counter_per_bay.

  Conditions: This symptom is observed from Cisco IOS interim Release 15.2(3.16)M0.1 on Cisco 5350 and Cisco 5400 routers.

  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= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 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 0x607F7154z
```

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T and Cisco IOS Release 15.1(4)M4. The issue is not observed with Cisco IOS Release 12.4(24)T6 or earlier releases. The issue occurs after reload.

  Workaround: Reapply the configuration after the router comes back up.

- CSCua40273

  Symptoms: The Cisco ASR 1000 router crashes when displaying MPLS VPN MIB information.

  Conditions: This symptom occurs on the Cisco ASR 1000 router with Cisco IOS Release 15.1(02)S.

  Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua40790

  Symptoms: Memory leaks when SNMP polling cbgpPeer2Entry MIB.

  Conditions: This symptom occurs when BGPv4 neighbors are configured.

  Workaround: There is no workaround if this MIB is to be polled.

- CSCua41398

  Symptoms: The Cisco SUP720 crashes.

  Conditions: This symptom occurs when you issue the **sh clns interface | i ^[A-Z]|** *Number of active* command multiple times via script with the following error and decodes:

```
%ALIGN-1-FATAL: Corrupted program counter 00:53:22 EET Tue Jun 5 2012
pc=0x0 , ra=0x411514F4 , sp=0x55A8B080

c7600s72033_rp-adventerprisek9-m.122-33.SRE5.symbols.gz read in
Enter hex value: 0x407F5B70 0x407F612C 0x407E026C 0x42BCA588 0x407EDDFC
0x41A78BB8 0x41A78B9C
0x407F5B70:get_alt_mode(0x407f5b68)+0x8
0x407F612C:get_mode_depth(0x407f6118)+0x14
0x407E026C:parse_cmd(0x407ded18)+0x1554
0x42BCA588:parser_entry(0x42bca360)+0x228
0x407EDDFC:exec(0x407ed344)+0xab8
0x41A78BB8:r4k_process_dispatch(0x41a78b9c)+0x1c
0x41A78B9C:r4k_process_dispatch(0x41a78b9c)+0x0
```

  Workaround: There is no workaround.

- CSCua42104

  Symptoms: CUBE with a transcoder generates malformed RTCP packets.

  Conditions: This symptom is observed with SIP-to-SIP CUBE with a transcoder registered to CUCM.

```
CIPC -- CUCM -- SIP -- CUBE -- SIP -- ITSP
CIPC -- G.729 -- CUBE (with transcoder) -- G.711 -- ITSP
```

  RTCP packets sent from ITSP are sometimes malformed when CUBE them sends to the originating device.

  Workaround: There is no workaround.

- CSCua42523

  Symptoms: The router crashes and reloads when “options-keepalive” is enabled on a dial peer which has the session target as sip-server.

  Conditions: This symptom is observed when enabling “options-keepalive” which has a session target as sip-server. Also, “sip-server” is configured under “sip-ua” and has a DNS address which resolves to an IPv6 address.

  Workaround: Do not enable “options-keepalive” for the dial peer.

- CSCua43930

  Symptoms: The checksum value parsed from the 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.

- CSCua44462

  Symptoms: DNS reply is not cached.

  Conditions: This symptom is observed with DNS-based X25 routing. The DNS server is reachable via IPsec over a Gigabit link and SHDSL links. There are Cisco devices at different locations. Few of communicate to the DNS server via IPsec over a Gigabit link and few of them communicate 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.

- 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.

- CSCua45548

  Symptoms: The router crashes with **show ip sla summary** on longevity testing.

  Conditions: This symptom is observed with Cisco 2900, 1900, and 3945 routers configured with IPSLA operations. The router which was idle for one day crashes on issuing the command **show ip sla summary**.

  Workaround: There is no workaround.

- CSCua45685

  Symptoms: A Cisco 2951, 3925, or 3945 crashes during rekey when GetVPN is configured and rekey packet size > MTU.

  Conditions: This symptom is observed if a rekey is coming through the interface where a crypto map is applied.

  Workaround: There is no workaround.

- CSCua46304

  Symptoms: A crash is seen at __be_nhrp_group_tunnel_qos_apply.

  Conditions: This symptom is observed when flapping a DMVPN tunnel on the hub in a scale scenario.

  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.

- CSCua48060

  Symptoms: A Cisco 3945 UUT router reloads after applying PPP and AAA authentication as well as authorization. The same issue is seen for other platforms, namely Cisco 1803 and Cisco 3845 for the same script.

Conditions: This symptom is observed when applying the AAA and PPP configurations with Cisco IOS interim Release 15.2(3.16)M0.1.

Workaround: There is no workaround.

- 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.

- CSCua50247

  Symptoms: Dropped ping packets on an NM-16ESW module.

  Conditions: This symptom is observed with ping packets with a size between 1501-1524 and between NM-16-ESW modules.

  Workaround: There is no workaround.

- CSCua50490

  Symptoms: Parts of the IOS configuration for the interface UCSE are not automatically applied onto the UCSE after a module OIR.

  Conditions: This symptom is observed after a module OIR or when a UCSE interface configuration is being changed while the module is not fully up and running.

  Workaround: Repeat the interface UCSE configuration in Cisco IOS after the module comes up completely.

- 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.

- CSCua53772

  Symptoms: The router crashes when scheduling a y1731 DMM IP SLA probe to run.

  Conditions: This symptom happens when the probe's target cfm mep is configured under service instance with double tag encapsulation.

  Workaround: There is no workaround.

- CSCua55785

  Symptoms: Build breakage is observed due to the fix of CSCtx34823.

  Conditions: This symptom occurs with the CSCtx34823 fix.

  Workaround: CSCtx34823 change may be unpatched from the code-base.

- CSCua55797

  Symptoms: The **privilege exec level 0 show glbp brief** command causes the memory to be depleted when the **show running** or **copy running-config startup-config** commands are used. The configurations will then show this:

```
privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
    privilege exec level 0 show glbp GigabitEthernet0/0 brief
    privilege exec level 0 show glbp
    privilege exec level 0 show
```

Removing the configurations causes this to happen over and over until the telnet session is terminated:

```
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
priv_push : no memory available
```

If the configurations are saved and device is reloaded, the device will not fully boot until the configurations are bypassed.

Conditions: This symptom occurs after the **privilege exec level 0 show glbp brief** command is entered and saved.

Workaround: Reload the router before saving the configurations.

- CSCua56184

  Symptoms: Multiple RP switchovers occur within a very short span of time.

  Conditions: This symptom is observed with multiple RP switchovers on a Cisco ASR 1000 router and it fails to allocate an IPsec SPI.

  Workaround: There is no workaround.

- CSCua56802

  Symptoms: QoS will not work on one of the subinterfaces/EVC.

  Conditions: This symptom occurs when HQoS policy is configured on more than one subinterface/EVC on ES+ and then add flat SG on them.

  Workaround: Remove and reapply SG.

- CSCua58100

  Symptoms: The syslog is flooded with the following traceback message:

  ```
  Jun 20 10:05:23.961 edt: %SYS-2-NOTQ: unqueue didn't find 7F3D26BDCCD8 in queue
  7F3CA5E4A240 -Process= "RADIUS Proxy", ipl= 0, pid= 223
  -Traceback= 1#e0ee0ce60492fdd11f0b03e0f09dc812  :400000+873623 :400000+2547652
  :400000+20F9217 :400000+6C70C9C :400000+6C69C71 :400000+6C682BC :400000+6C68183
  ```

  Conditions: This symptom occurs under the following conditions:

  - You establish 36k EAPSIM sessions using a RADIUS client on server A.
  - You establish 36k roaming sessions using a RADIUS client on server B.
  - The roaming sessions have the same caller-station-id but use a different IP address than the EAPSIM sessions.

  Workaround: There is no workaround.

- CSCua60100

  Symptoms: The router crashes at ip_acl_peruser_ctxt_free while clearing the calls.

  Conditions: This 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.

- 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.

- CSCua61814

  Symptoms: Overhead accounting configuration needs to be configured on both the parent and child policy, rather than just the parent.

  Conditions: This symptom is observed with overhead accounting.

  Workaround: There is no workaround.

- CSCua63182

  Symptoms: Incorrect minimum bandwidth is displayed when 0k bandwidth is received from a peer of a different version.

  Conditions: This symptom occurs under the following conditions:

  - Different behavior in Cisco ASR code when the bandwidth for a route is very high, that is, more than 10G.
  - Cisco IOS XE Release 2.6.2 and earlier releases send 0K when the bandwidth for a route is more than 10G.
  - Cisco IOS XE Release 2.6.2 and earlier releases use incoming interface bandwidth, when BW = 0 is received.
  - Cisco IOS XE Release 3.4.3S and later releases send the real bandwidth, even if it is more than 10G.
  - Cisco IOS XE Release 3.4.3S and later releases use the lesser value between “received bandwidth” and “incoming interface bandwidth”.
  - Cisco IOS XE Release 3.4.3S and later releases convert incoming bandwidth to 1K in case BW = 0 received.
  - When the peers are of the same or compatible version, that is, both peers are Cisco IOS XE Release 2.6.2 and earlier releases or both peers are Cisco IOS XE Release 3.4.3S and later releases, there is no issue. However, when the peers are of different or incompatible version, that is, one peer is Cisco IOS XE Release 2.6.2 or an earlier release and the other peer is Cisco IOS XE Release 3.4.3S or a later release, then this issue is seen.

  Workaround: There is no workaround.

- CSCua63440

  Symptoms: A crash is seen on executing **show metadata flow local-flow-id** *id*.

Conditions: This symptom is observed when “metadata flow” is configured and metadata flows are present in the metadata table.

Workaround: There is no workaround.

- CSCua64100

  Symptoms: SCTP receives message fails.

  Conditions: This symptom occurs when sock-test testing infrastructure is used for SCTP testing.

  Workaround: Use another test tool for SCTP testing. Issue is in sock-test. Not in SCTP.

- CSCua65278

  Symptoms: Modem disappears with the **cellular 0 cdma mode evdo** command.

  Conditions: This 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.

- CSCua66908

  Symptoms: Build fails on Cisco IOS Release 15.3M&T.

  Conditions: This symptom was observed after the commit of CSCua06101 due to unnecessary duplication of a line.

  Workaround: Remove the line before building.

- 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.

- CSCua69657

  Symptoms: Traceback is seen when executing the **show clock detail** command.

  Conditions: This symptom is seen when executing the **show clock detail** command with Cisco IOS interim Release 15.3(0.4)T image.

  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.

- CSCua70158

  Symptoms: NBAR fails to recognize traffic with **match protocol http url/host**.

  Conditions: This symptom is seen when “protocol discovery” is enabled.

  Workaround: There is no workaround.

- CSCua70738

  Symptoms: Ping between UUT and peer does not work.

  Conditions: This symptom is observed with a simple IP and PVC configuration under both UUT and the peer’s ATM interface.

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

- CSCua73419

  Symptoms: Transform set including SHA2 does not work on ISM.

  Conditions: This symptom is observed with esp-sha256-hmac, esp-sha384-hmac, or esp-sha512-hmac.

  Workaround: There is no workaround.

- CSCua75781

  Symptoms: CME reloads for E911 call ELIN translation for incoming FXS/FXO trunk.

  Conditions: This symptom is observed from Cisco IOS interim Release 15.3(0.2)T.

  Workaround: There is no workaround.

- 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?a
ction=search&counter=0&paging=5&links=reference&index=all&query=SYS-5-SCHEDULED_RELOAD
>
Reload requested for 13:56:51 UTC Mon May 21 2012 at 13:46:51 UTC Mon May 21
2012 by console. Reload Reason: Reload Command.
```

  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.

- CSCua79446

  Symptoms: Building Cisco c3900/c2900 images is not possible due to double commit of DDTS CSCtb88203.

  Conditions: This symptom occurs due to the double commit of DDTS CSCtb88203, which impacts H323 ISSU.

  Workaround: There is no workaround.

- CSCua82425

  Symptoms: A Cisco router may unexpectedly reload when using EMM when choosing a menu option that executes “reload” or “do reload”.

  Conditions: This symptom occurs if there are unchanged configuration changes.

  Workaround: Change the menu option to save the configuration before the reload. If you do not want to save the configuration, then there is no currently known workaround.

  Further Description: In the newer code, the crash does not occur with “do reload” (though “reload” still crashes), but it still does not result in the desired behavior or reloading the device.

- CSCua84879

  Symptoms: A crash is seen at slaVideoOperationPrint_ios.

  Conditions: This symptom is observed when IPSLA video operations are configured and **show running-config** is issued.

  Workaround: There is no workaround.

- 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 queuing features are used.

  Conditions: This symptom is observed with the following conditions:

  1. The issue must have the user-defined queue-limit defined.
  2. This error recovery defected is confirmed as a side effect with the c3pl cnh component project due to ppcp/cce infrastructure enhancement.

  Workaround: There is no workaround.

- CSCua85239

  Symptoms: Flapping BGP sessions are seen if large BGP update messages are sent out and BGP packets are fragmented because midpoint routers have the smaller “mtu” or “ip mtu” configured.

```
*Jun  3 18:20:20.792 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:30.488 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:36.451 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP
Notification sent
*Jun  3 18:20:36.451 UTC: %BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0
(hold time expired) 0 bytes
```

```
*Jun  3 18:20:36.569 UTC: %BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4
Unicast topology base removed from session  BGP Notification sent
*Jun  3 18:20:40.184 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:44.619 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up
*Jun  3 18:20:49.926 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:59.604 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
```

Conditions: This symptom is observed between two BGP peers with matching MD5 passwords configured and can be triggered by the following conditions:

- If the midpoint path has the “mtu” or “ip mtu” setting that is smaller than the outgoing interface on BGP routers, it will be force the BGP router to fragment the BGP packet while sending packets through the outgoing interface.
- Peering down and the MD5 error do not always occur. They occur only once or twice within 10 tests.

Workaround: There is no workaround.

- CSCua85934

  Symptoms: A session provisioning failure is seen in the ISG-SCE interface. The deactivate or disconnect request has the message authenticator wrongly calculated.

  Conditions: This symptom is observed with the ISG-SCE interface.

  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.

- CSCua91104

  Symptoms: ISIS adjacency process shows traceback messaging related to managed timer.

  Conditions: This symptom is observed when configuring isis network point-to-point on LAN interface with isis bfd or isis ipv6 bfd enabled. The traceback does not happen always. It depends on timing.

  Workaround: Disable isis bfd or isis ipv6 bfd before issuing the **isis network point-to-point** command. Restore the isis bfd or isis ipv6 bfd configuration on the LAN interface.

- CSCua91473

  Symptoms: Memory leak occurs during rekey on the IPsec key engine process.

  Conditions: This symptom occurs after rekey, when the IPsec key engine does not release KMI memory, causing the IPsec key engine holding memory to keep increasing.

  Workaround: Clear crypto session for IPsec key engine to release memory.

- CSCua91698

  Symptoms: ephone-type disappears from the running-configuration.

  Conditions: This symptom occurs in SRST mode and after reload.

  Workaround: Reconfigure the ephone-type commands and again save to startup-configuration.

- CSCua93688

  Symptoms: When pinging from the Cisco 1921 router to connected devices, the response time is unexpectedly slow.

  ```
  round-trip min/avg/max = 8/46/92 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.

- CSCua94334

  Symptoms: Hung calls are seen on CME. Hung calls seen in "show call active voice brief" are as follows:

  ```
  1502 : 26 36329310ms.1 +-1 pid:1 Answer XXXYYY4835 connected
  dur 00:00:00 tx:0/0 rx:0/0
  IP 0.0.0.0:0 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729r8
  pre-ietf TextRelay: off
  media inactive detected:n media contrl rcvd:n/a timestamp:n/a
  long duration call detected:n long duration call duration:n/a timestamp:n/a
  ```

  Conditions: This symptom is observed when an inbound H225 call setup request to a CME gateway results in a hung call if a release complete is received while still in alerting state. This issue occurs only when the shared line is configured on the phone and the shared line is not registered.

  Workaround: Remove the shared line or register the shared line.

- CSCua94947

  Symptoms: RP crashes when downloading FreeRadius Framed-IPv6-Route on MLPPP sessions.

  Conditions: This symptom occurs when downloading radius Framed-IPv6-Route.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCua97209

  Symptoms: The **analysis-module** CLI is missing under "interface GigabitEthernet".

  Conditions: This symptom is observed with Cisco ISRs running a Cisco IOS Release 15.2(4)M image with either SRE or UCSE modules inserted and the module software publish NAM subsystem capability.

  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.

- CSCua98902

  Symptoms: fibidb is not getting intialized.

  Conditions: This symptom is observed when LFA FRR is configured in Cisco ME 3800x and ME 3600x switches.

  Workaround: There is no workaround.

- CSCua99687

  Symptoms: BFD does not come up with Zone-Based Firewall (ZBFW) applied on the same interface.

  Conditions: This symptom is observed when BFD and ZBFW are configured on a Gigabit interface on a Cisco CGR 2010 running Cisco IOS Release 15.1(4)M4. It works fine on Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCub02830

  Symptoms: The **analysis-module** command is missing under the Gigabit Ethernet interface even when the UCS E-Series Server module has the publish NAM subsystem type.

  Conditions: This symptom occurs on Cisco ISRs running a Cisco IOS 15.2(4)M image with UCS E-Series Server modules inserted and the module software publish NAM subsystem capability.

  Workaround: There is no workaround.

- CSCub04112

  Symptoms: The router may lose OSPF routes pointing to the reconfigured OSPF interface.

  Conditions: This symptom occurs after quick removal and adding of the interface IP address by script or copy and paste.

  For example, configure the following:

```
interface Ethernet0/0
 ip address 1.1.100.200 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
end
```

  Then, quickly remove/add the IP address:

```
conf t
interface Ethernet0/0
 no ip address 1.1.100.200 255.255.255.0
 ip address 1.1.100.200 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
end
```

  Workaround: Insert a short delay in between commands for removing/adding the IP address. The delay should be longer than the wait interval for LSA origination; by default, it is 500 ms. Or, refresh the routing table by “clear ip route *”.

- CSCub04345

  Symptoms: Cisco ASR-1002-X freezes after four hours with a scaled “path-jitter” sla probe configuration.

  Conditions: This symptom is observed with a scaled “path-jitter” sla probe configuration.

  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.

- CSCub06131

  Symptoms: The IPSLA sender box can reload with the following message:

  ```
  SYS-6-STACKLOW: Stack for process IP SLAs XOS Event Processor running low, 0/6000
  ```

  Conditions: This symptom is observed with the IPSLA sender box.

  Workaround: There is no workaround.

- CSCub06859

  Symptoms: OSPFv2 NSR on quad-sup VSS does not work. The router stops sending hello packets after switchover.

  Conditions: This symptom is observed with quad-sup VSS with OSPFv2 NSR.

  Workaround: Clear the IP OSPF process after NSR switchover.

- CSCub07382

  Symptoms: NHRP cache entry for the spokes gets deleted on NHRP hold timer expiry even though there is traffic flowing through the spoke-to-spoke tunnel.

  Conditions: This symptom is observed with a flexVPN spoke-to-spoke setup.

  Workaround: Configure the same hold time on both tunnel interface and the virtual-template interface.

- CSCub07673

  Symptoms: IPsec session does not come up for spa-ipsec-2g if ws-ipsec3 is also present. “Volume rekey” is disabled on Zamboni.

  Conditions: This symptom occurs if we have “volume rekey” disabled on Zamboni.

  Workaround: Do not disable the volume rekey on Zamboni.

- CSCub07855

  Symptoms: The VRF error message is displayed in the router.

  Conditions: This symptom occurs upon router bootup.

  Workaround: There is no workaround.

- CSCub09124

  Symptoms: MDT tunnel is down.

  Conditions: This symptom is seen in MVPN. If the **ip multicast boundary** command on non-current RPF interface blocks the MDT group, it may cause MDT tunnel failure.

Workaround: Adding the **static join** command under PE loopback interface may work around the problem temporarily.

- 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.

- CSCub13317

  Symptoms: The Cisco 2900 with VWIC2-2MFT-T1/E1 in TDM/HDLC mode does not forward any traffic across the serial interface after a certain amount of time.

  Conditions: This symptom is observed when frame relay is configured over VWIC2 channel-group in TDM/HDLC mode.

  Workaround: Configure VWIC2 channel-group in NMSI mode.

  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: 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:OF/RC:C

  CVE ID CVE-2012-3918 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

- CSCub14044

  Symptoms: A crash with traceback is seen, and all calls are dropped.

  Conditions: This symptom is observed under all conditions.

  Workaround: There is no known workaround. The gateway crashes, and the soak time appears to be six weeks.

- CSCub14299

  Symptoms: The router reloads when “no mediatrace initiator” is issued.

  Conditions: This symptom occurs when traceroute is enabled for a mediatrace session.

  Workaround: Disable traceroute under each configured mediatrace session.

- CSCub16372

  Symptoms: In extremely rare cases, an 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: This symptom occurs when all the following three 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 occur, so far only one CCO image is found to have this problem.

  Workaround: Upgrading ROMmon to the latest version of 15.0(1r)M16 or 151(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 CCO. For example, C3900_RM2.srec.SPA.150-1r.M16 is the
latest ROMMON version for C39xx platforms located at CCO download site:
http://www.cisco.com/cisco/software/release.html?
mdfid=282774222&flowid=7437&softwareid=280805687&release=15.0%281r%
29M16&relind=AVAILABLE&rellifecycle=&reltype=latest.
```

- CSCub17985

  Symptoms: A memory leak is seen when IPv6 routes are applied on the per-user sessions.

  Conditions: This symptom is seen if IPv6 routes are downloaded as a part of the subscriber profile. On applying these routes to the sessions, a memory leak is observed.

  Workaround: There is no workaround.

- CSCub19471

  Symptoms: A crash occurs during bootup with MACE and SNMP configurations.

  Conditions: This symptom is observed when the startup configuration contains MACE type (policy-map type mace) configured with both filter (match access-group) and action (except flow monitor). The SNMP configuration is as follows:

```
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 the SNMP configuration.

- CSCub21340

  Symptoms: A segmentation fault crash is seen and the router reloads continuously.

  Conditions: This symptom occurs when a router is reloaded with CFM over an xconnect scale configuration (configuring 500 meps).

  Workaround: There is no workaround.

- CSCub24355

  Symptoms: IPv4 mVPN inactive (S,G) are not removed on the egress PE.

  Conditions: This symptom occurs when you stop traffic, causing the timers to stop.

  Workaround: Remove entries manually.

- 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.

- CSCub31477

  Symptoms: A Cisco ISG router configured for Layer 2 Connected Subscriber Sessions does not respond to ARP replies once a subscriber ARP cache has expired.

  Conditions: This symptom occurs when the router is configured as ISG L2-Connect, the router has configured HSRP as the high-availability method, and the subscriber-facing interface is configured with “no ip proxy arp”. This issue is not seen if either HSRP is removed or if “ip proxy arp” is enabled.

  Workaround: Clear the subscriber session. After the subscriber is reintroduced, the issue is resolved. You can also configure “ip proxy arp” on the HSRP-configured interface.

- CSCub32500

  Symptoms: The router crashes in EIGRP due to chunk corruption.

Conditions: This symptom is observed on EIGRP flaps.

Workaround: There is no workaround.

- CSCub33877

  Symptoms: During “issue loadversion”, when downgrading from Texel (or later) to Yap (v151_1_sg_throttle or earlier), the standby RP keeps reloading due to the out of sync configuration.

  Conditions: This symptom occurs during the “issu loadversion” operation. The newer version of the image supports IPv6 multicast while the older version of image does not.

  Workaround: There is no workaround.

- CSCub39124

  Symptoms: Only secure cookies will be sent to HTTPS (HTTP over SSL) servers. If secure is not specified, a cookie is considered safe to be sent in the clear over unsecured channels.

  Conditions: This symptom is the current default behavior.

  Workaround: There is no workaround.

  Further Problem Description: This defect has been opened to ensure that the default value of the WebVPN cookie is hardened and includes the secure keyword as per RFC 2109.

- CSCub39268

  Symptoms: Cisco ASR 1000 devices running an affected version of Cisco IOS XE are vulnerable to a denial of service vulnerability due to the improper handling of malformed IKEv2 packets. An authenticated, remote attacker with a valid VPN connection could trigger this issue, resulting in a reload of the device. Devices configured with redundant Route Processors may remain active as long as the attack is not repeated before the affected Route Processor comes back online.

  Conditions: This symptom occurs when Cisco ASR1000 devices are configured to perform IPsec VPN connectivity. Devices running an affected version of Cisco IOS XE are affected. Only an authenticated IKEv2 connection is susceptible to this vulnerability.

  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 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-5017 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

- CSCub42181

  Symptoms: The router crashes continuously after a normal reboot due to power or some other reason.

```
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M4,
RELEASE SOFTWARE (fc1)
 uptime is 4 days, 11 hours, 38 minutes
System returned to ROM by error - a Software forced crash, PC 0x88D26F0 at
07:42:45 UTC Sat May 5 2012
System restarted at 07:43:55 UTC Sat May 5 2012
System image file is "flash:c3900-universalk9-mz .SPA.150-1.M4.bin" ;
Last reload type: Normal Reload
----------------------------
generated Traceback:

Pre Hardware Replacement Crashinfo:
```

```
-----------------------------------
#more flash0:crashinfo_20120519-165015-UTC

------------------
Traceback Decode:
------------------

tshakil@last-call-2% rsym c3900-universalk9-mz.150-1.M4.symbols.gz
Uncompressing and reading c3900-universalk9-mz.150-1.M4.symbols.gz via
/router/bin/zcat
c3900-universalk9-mz.150-1.M4.symbols.gz read in
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c

0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
Enter hex value:


--------------------------------
Crash File Post Installation:
------------------------------

#more flash0:crashinfo_20120519-185725-UTC


------------------
Traceback Decode:
-----------------

Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4
Enter hex value: 0x88D1D88z 0x88D27C0z 0x729E558z 0x729E6F4z 0x495F298z 0x4962FC8z
0x88D1D88:fsm_crank(0x88d1d2c)+0x5c
0x88D27C0:fsm_exec_w_option(0x88d2650)+0x170
0x729E558:htsp_process_event(0x729e1d4)+0x384
0x729E6F4:htsp_main(0x729e62c)+0xc8
0x495F298:ppc_process_dispatch(0x495f274)+0x24
0x4962FC8:process_execute(0x4962e24)+0x1a4

-------------------------------------------------
```

Conditions: This symptom is observed with the following conditions:

- MGCP gateway.
- Take out all the modules from the router.
- Put the modules one by one.

- Apply the configuration.
- The router is stable.

The lab test is recreated as follows:

1. Disable auto-configuration, that is, “no ccm-manager config” .
2. Reload the gateway.
3. Enable the CCM manager configuration and the router does not crash.

Workaround 1: Bypass the start-up configuration and log in via ROMmon without any configuration. Add the configuration one by one. Once the configuration is added, save the configuration and reload the gateway.

Workaround 2: Shut down the router and add the cards one by one in slots 0, 1, 2, 3, and 4. The device is stable until the third slot is inserted and brought up. As soon the router is powered on, after adding the fourth slot, the crash starts. Shut down the router and remove the card in slot 4 (EVM-HD-8FXS/DID). Bring the device up without the card in slot 4 (EVM-HD-8FXS/DID). Remove the “mgcp” and “ccm-manager fallback-mgcp” configuration from the device because the console log is displaying the “Call Manager backhaul registration failed” error message. Shut down the router and add the card which was removed. Bring up the router. Readd the **ccm-manager fallback-mgcp** command and do a “no mgcp/mgcp”. The router becomes stable.

Workaround 3: Remove the **ccm-manager config** command by no ccm-manager config which tears down the connection from the call manager to the MGCP gateway. The gateway will not download the configuration from the call agent at the time of startup. Reload the router. Once the router is back and stable, readd the command.

- CSCub42920

  Symptoms: Keyserver rejects rekey ACK from GM with message (from **debug crypto gdoi ks rekey all**):

  ```
  GDOI:KS REKEY:ERR:(get:0):Hash comparison for rekey ack failed.
  ```

  The keys and policies in the rekey packet are correctly installed by the GM, but the rekey ACK does not get processed by the keyserver. This leads to rekey retransmissions, GM reregistration, and potential disruption of communication.

  Conditions: This symptom is observed when rekey ACK validation in versions Cisco IOS Release 15.2(4)M1 (Cisco ISR-G2) and Cisco IOS Release 15.2(4)S/Cisco IOS XE Release 3.7S (Cisco ASR 1000) is incompatible with other software releases.

  A keyserver that runs Cisco IOS Release 15.2(4)M1 or Cisco IOS Release 15.2(4)S/Cisco IOS XE Release 3.7S will only be able to perform successful unicast rekeys with a GM that runs one of those two versions. Likewise, a keyserver that runs another version will only interoperate with a GM that also runs another version.

  Workaround: Use multicast rekeys.

- CSCub43088

  Symptoms: The following console messages are seen:

  ```
  Delayed UCSE configuration: Wrong module type in slot 2
  ```

  whenever the SRE-SM modules register with IOS version:

  c2951-universalk9-mz.SPA.152-4.M.

  Conditions: This symptom is observed when you have SM-SRE modules register with the router via RBCP. Typically when the application on the module boots up or when the you issue SRE **sm status** command in IOS.

Workaround: There is no workaround.

Further Problem Description: This is a benign message and can be ignored.

- CSCub45763

  Symptoms: The switch may crash following SYS-2-FREEFREE and SYS-6-MTRACE messages while a CDP frame is being processed.

  Conditions: This symptom occurs when the switch is running Cisco IOS Release 12.2(53)SG7 and has CDP enabled.

  Workaround: Disable CDP using “no cdp run”.

- CSCub45809

  Symptoms: Cisco IOS configured for Voice over IP may experience stack corruption due to multiple media loops.

  Conditions: This symptom requires a special configuration of IP features, along with disabling the recommended **media flow-around** command. This issue is seen with Cisco IOS Release 15.2(2)T.

  Workaround: Issue the **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

- CSCub46423

  Symptoms: Connecting from Windows 7 L2TP/IPSec client to the VPN fails when using HSRP virtual IP as a gateway IP and Error 788 is displayed.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T or later releases, and the Windows 7 L2TP/IPsec VPN client.

  Workaround: Downgrade to Cisco IOS Release 15.1(3)T.

- 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.

- CSCub47910

  Symptoms: Unexpected reboot is seen due to a cBus Error when using 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.

- CSCub49291

  Symptoms: Static tunnels between hubs and spokes fail to rebuild.

  Conditions: This symptom is observed when you reload the hub on the DMVPN IPv6 setup with DPD on-demand enabled on all spokes.

Workaround: There is no workaround.

- CSCub51862

  Symptoms: The router crashes when MACE is applied to an interface and traffic is sent through that interface.

  Conditions: This symptom is observed when there is no flow record configured inside any of the MACE flow monitors.

  Workaround: Configure flow records and exporter inside the MACE flow monitors.

- CSCub52892

  Symptoms: The options “log” and “reset” are not configurable in the URL filter policy. The existing configuration is removed if upgrading from previous/good releases.

  Conditions: This symptom is observed with the options “log” and “reset” in the URL filter policy.

  Workaround: There is no workaround.

- CSCub52943

  Symptoms: When executing Media Forking with midcall codec change, memory leaks are found in Cisco ASR for CCSIP_SPI_CONTROL. After decoding, the memory leak is found to be for the function is_x_participant_sips() as it is not releasing the memory after allocated with some memory. This seems to be a side effect of one of the DDTS that was committed to Cisco IOS Release 15.3M&T (CSCtz96408).

  Conditions: This symptom occurs when executing Media Forking with midcall codec change.

  Workaround: The fix is done and is committed to Cisco IOS Release 15.3M&T.

- CSCub54872

  Symptoms: A /32 prefix applied to an interface (for example, a loopback) is not being treated as connected. This can impact the connectivity of the /32 prefix.

  Conditions: This 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.

- CSCub55297

  Symptoms: The CEM interface (Serial Interface Network Modules - NM-CEM-4SER and NM-CEM-4TE1) does not come up with the latest Cisco IOS Release 15.3(1)T image.

  Conditions: This symptom is observed with Cisco IOS Release 15.3(1)T.

  Workaround: There is no workaround.

- CSCub58932

  Symptoms: PA export times shift one minute ahead after a certain period of time. For example, instead of exporting at times 5:00, 5:05, 5:10, 5:15 (a 5-minute interval), the export times are shifted to 4:59, 5:04, 5:09 etc.

  Conditions: The conditions are unknown.

  Workaround: There is no workaround. A countermeasure would be restart the PA timer by reissuing the **cache timeout update ...** command. This will likely remedy the issue.

- CSCub59493

  Symptoms: The CPU remains at 100% after the SNMPv 2c walk even after 5 minutes.

Conditions: This symptom occurs when an SNMP walk is done on mplsLsrStdMIB.

Workaround: There is no workaround.

- CSCub62116

  Symptoms: Traceback is seen when sending HTTP traffic.

  Conditions: This symptom is observed when MACE is enabled on an interface. After several minutes, traceback is seen.

  Workaround: There is no workaround.

- CSCub62729

  Symptoms: MTU-Size issue is seen with ppp-max-payload enabled.

  Conditions: This symptom occurs when ppp-max-payload is enabled in Cisco c887VA (with ppp-max-payload enabled).

  Workaround: There is no workaround. The same configuration works fine in Cisco c881/c1921.

- CSCub67243

  Symptoms: The router crashes under heavy traffic when configured as DMVPN HUB. No crashinfo or core file is generated.

  Conditions: This symptom is observed on a Cisco 3900e router, but not on a Cisco 3900 router.

  Workaround: Configure “no scheduler allocate”.

- CSCub71162

  Symptoms: The VLAN interface is not working.

  Conditions: This symptom occurs because of a change in the netmask.

  Workaround: Shut/no shut resolves the interface.

- CSCub71981

  Symptoms: The **show voice register pool on-hold brief** command displays the same number (for both phone number and remote number) when both local and remote phone are put on on-hold.

  Conditions: This symptom is observed when with Cisco IOS Release 15.3(8)T.

  Workaround: There is no workaround.

- CSCub78299

  Symptoms: Ping fails from host1 (192.168.1.2) to host2 (192.168.4.2).

  Conditions: This symptom occurs when Suite-B is configured on IPsec SA.

  Workaround: There is no workaround.

- CSCub79590

  Symptoms: The **match user-group** commands do not appear in the running configuration after being configured.

```
Configure an inspection type class-map:
class-map type inspect TEST
    match protocol tcp
    match user-group cisco

Save the configuration. Try to view the configuration in the running configuration:
hostname# show run class-map
building configuration...

Current configuration : 66 bytes
```

```
!
class-map type inspect match-all TEST
   match protocol tcp
end
```

But, view the configuration directly in the class-map:

```
hostname# show class-map type inspect
   Class Map type inspect match-all TEST (id 1)
     Match protocol tcp
     Match user-group cisco
```

The configuration never shows up in the running configuration, but it is in the class-map configuration. As a note, the functionality exists on the ZBFW, but the configuration does not show up in the running configuration.

Conditions: This symptom is only observed with the **match user-group** commands.

Workaround: This issue only affects devices after a reload as the router will read the startup configuration, which will not have the **match user-group** command. As a result, the **match user-group** commands need to be reentered after ever reload.

- CSCub80491

  Symptoms: A Cisco router may experience alignment errors. These alignment errors may then cause high CPU.

  Conditions: This symptom occurs as the alignment errors require using Get VPN. It is currently believed to be related to having the Get VPN running on a multilink interface, but this is not yet confirmed.

  Workaround: There is no workaround.

- 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.

- CSCub85754

  Symptoms: Ping does not work on a Cisco 897VA.

  Conditions: This symptom is observed with an upgrade to 37h DSL firmware.

  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.

- CSCub91111

  Symptoms: Outgoing packet drop on the HSPA+R7 cellular interface with SWI MC8705 firmware T3.5.x (not released).

  Conditions: This symptom is observed on HSPA+R7 SKU with MC8705 T3.5 firmware (not released firmware).

  Workaround: Use MC8705 firmware T1.x release.

- 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.

- CSCub93496

  Symptoms: One-way video from CTS-1000 to TS-7010 is seen in the following topology:

  ```
  CTS-1000 (v1.9.1) >>> CUCM 8.6.2aSU2 >>> CUCM 9.0 >>> CUBE 15.1.2T (2811) >>>
  CUBE 15.1.4M4 (2951) >>> CUCM9.0 >>> VCS X7.1 >>> TS-7010 2.2
  ```

  Conditions: This symptom occurs when SDP Passthru mode on CUBE is used.

  Workaround: RTP payload types 96/97, which are associated with fax/faxack need to be remapped to some other unused values.

- CSCub94825

  Symptoms: After Cisco IOS XE bootup, there are no static reverse routes inserted as a result of applying/installing and HA crypto map. The same issue is present on the HSRP standby device, namely, the static RRI routes will not get installed in case a failover occurs. The **show cry map** command can be used to verify that RRI is enabled. The **show cry route** command can be used to determine if RRI has happened and if it has been done correctly.

  Conditions: This symptom is observed with the following conditions:

  - Cisco IOS XE Release 3.5S up to Cisco IOS XE Release 3.7S
  - VRF-aware IPSec with stateless HA and static RRI
  - IPv4

  Workaround: Removing and reentering the **reverse-route static** command into the the configuration will actually trigger the route insertion.

- CSCub99756

  Symptoms: The Cisco ASR 1000 router running Cisco IOS Release 15.2(4)S acting as a GM in a Get VPN deployment starts using the most recent IPsec SA upon KS rekey instead of using the old key up to 30 seconds of expiration.

  Conditions: This symptom is observed only in Cisco IOS Release 15.2(4)S.

  Workaround: There is no workaround.

- CSCub99778

  Symptoms: The Cisco ASR 1000 router being GM in a Get VPN deployment fails to start GDOI registration after a reload.

  Conditions: This symptom occurs when running Cisco IOS Release 15.2(4)S. The following error is displayed in the **show crypto gdoi** command output after reload.

  ```
  Registration status   : Not initialized
  ```

  Workaround: Use an EEM script to issue “clear crypto gdoi” some time after boot time or issue this manually.

- CSCuc05631

  Symptoms: Tracebacks are seen in the ISM-VPN background.

Conditions: This symptom is observed when Get VPN and DMVPN are turned by having the ISM-VPN Module.

Workaround: Disable ISM-VPN and use the onboard VPN ACCL.

- 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.

- CSCuc08061

  Symptoms: IPv6 DMVPN spoke fails to rebuild tunnels with hubs.

  Conditions: This symptom occurs when the tunnel interface on the spoke is removed and reapplied again.

  Workaround: Reboot the spoke.

- CSCuc12907

  Symptoms: The **waas config remove-all** and **waas config restore-default** commands fail.

  Conditions: This symptom occurs when the **waas config remove-all** and **waas config restore-default** commands fail. WAAS-Express class-maps, policy-maps, and parameter-map fail to be removed when the previous commands are issued. The following error is seen:

  ```
  % Remove All Config failed: Unable to remove WAAS class-map(s).
  ```

  Workaround: On Cisco c3900, c2951, c2900, and c1900, install the datak9 package. The CLIs are successful then.

- CSCuc15203

  Symptoms: If the ISM-VPN module is turned on and ZBFW is configured, when asymmetric routing occurs, the router crashes.

  Conditions: This symptom occurs when the ISM-VPN module is turned on and ZBFW is configured, and when asymmetric routing occurs.

  Workaround: There is no workaround.

- CSCuc15695

  Symptoms: The counters are not polling the correct stats.

  Conditions: This symptom was first observed on the ATM interfere, but it is not particular to the ATM as this issue was reproduced on the Gigabit Ethernet interface as well.

  Workaround: There is no workaround.

- CSCuc24937

  Symptoms: The voice gateway router is configured as a CME for handling ephone reloads due to spurious memory access.

  Conditions: This symptom occurs as the voice gateway router is capable of handling ephones. Reload is very specific to ephone handling.

  Workaround: There is no workaround.

- CSCuc29310

  Symptoms: TD probes in fast mode are gone when the link flaps (not PfR external interfaces).

  Conditions: This symptom is observed with TD, fast mode, and link flap, which cause SAF session flap.

Workaround: Issue “clear pfr mas tr”.

- CSCuc33328

  Symptoms: Memory leaks are seen in the statistics.

  Conditions: This symptom occurs when the probe is executed and statistics are updated.

  Workaround: There is no workaround.

- CSCuc37365

  Symptoms: The **bandwidth** command under the cellular interface goes back to the default bandwidth of 50K after a reload or modem reset/power-cycle.

  Conditions: This symptom is observed when you configure the **bandwidth** command.

  Workaround: There is no workaround.

- CSCuc37407

  Symptoms: If configuration replace is tried after session-based poll, which has an address type (IPv4/IPv6) mismatch with initiator source-IP, then a crash is seen.

  Conditions: This symptom occurs when configuring Mediatrace initiator with a particular type of address, for example, IPv4 only or IPv6 only. This issue is seen when trying a session-based poll with the address type for a path-specifier not matching the address type of the initiator. Then, configuration replace on the same configurations leads to a crash.

  Workaround: There is no workaround.

- CSCuc39963

  Symptoms: Spurious memory access/crash is seen at mdb_tree_classify.

  Conditions: This symptom occurs when the egress QoS policy is configured.

  Workaround: There is no workaround.

- CSCuc40448

  Symptoms: No-way audio is observed on hair-pinned calls back from CUBE to SIP Provider.

  The call flow is as follows:

  ```
  PSTN caller --Verizon---(sip)---ASR CUBE---(sip)---CUSP---(sip)---Genesis ( SIP
  Refer sent to transfer back to Verizon) -- CUSP - CUBE - Verizon -- PSTN
  ```

  Conditions: This symptom is observed only after upgrading to Cisco IOS Release 15.2(2)S.

  Workaround: Modify the diversion header on the transfer leg invite, so Verizon handles the call differently.

- CSCuc41531

  Symptoms: Forwarding loop is observed for some PfR-controlled traffic.

  Conditions: This symptom is observed with the following conditions:

  – Traffic Classes (TCs) are controlled via PBR.

  – The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class ...** command (this fixes the issue until the next occurrence).

- CSCuc45115

  Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.

  Conditions: This symptom is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

  Workaround: There is no known 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.

- CSCuc59541

  Symptoms: Spoke fails to learn networks behind other spokes and EIGRP flapping occurs.

  Conditions: This symptom is observed with a FlexVPN spoke-to-spoke setup.

  Workaround: There is no workaround.

- CSCuc66122

  Symptoms: A crash occurs with the **show ip sla summary** command with the IP SLAs RTP-Based VoIP Operation.

  Conditions: This symptom occurs when the IP SLAs RTP-Based VoIP Operation is configured on the box.

  Workaround: Use the **show ip sla statistics** command to check the status and statistics of the IP SLAs RTP-Based VoIP Operation rather than **show ip sla summary** command, when the IP SLAs RTP-Based VoIP Operation is configured on the box.

- CSCuc68743

  Symptoms: A crash occurs while running CME smoke regression.

  Conditions: This symptom is observed while running CME smoke regression.

  Workaround: There is no workaround.

- CSCuc70310

  Symptoms: RRI routes are not installed in DMAP. “reverse-route” is a configuration in the DMAP. This prevents packets from being routed through the intended interface, and hence packet loss occurs.

  Conditions: This symptom is observed when a simple reverse-route is configured in DMAP without any gateway options.

  Workaround: There is no workaround.

- CSCuc73677

Symptoms: RSA keys are not generated correctly.

Conditions: This symptom occurs when you first clear the RSA keys that are already generated on the router, and then generate the RSA keys.

Workaround: There is no workaround.

- CSCuc82992

  Symptoms: The router crashes upon execution of “no crypto engine slot 0”. when RG-infr feature is enable.

  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.

- CSCuc88175

  Symptoms: When a dynamic cryptomap is used on the Virtual Template interface, SAs do not created and thus the testscripts fail. This issue occurs because the crypto map configurations are not added to the NVGEN, and hence there is no security policy applied on the Virtual Template interface.

  Conditions: This symptom occurs only when a dynamic map is used on the Virtual Template interface. However, this issue is not seen when tunnel protection is used on the Virtual Template interface or when a dynamic map is used on the typical physical interface.

  Workaround: There is no workaround apart from using tunnel protection on the Virtual Template interface.

- CSCuc95573

  Symptoms: A call with the VCC feature enabled does not work properly, resulting in media problems, when DSP is not configured. The inleg sends all the codecs configured, even though DSP is not configured. It should send only the codecs negotiated on the outleg.

  Conditions: This symptom occurs when DSP is not configured. Configure VCC offer all in the dial peer.

  Workaround: Only negotiated codecs are sent out in 200 OK from the inleg when DSP resource is unavailable.

- CSCud07504

  Symptoms: SRE-WAAS optimized traffic gets dropped by ZBFW.

  Conditions: This symptom occurs when ZBFW, WCCP, and SRE-WAAS are configured.

  Workaround: There is no workaround.

# Related Documentation

The following sections describe the documentation available for Cisco IOS Release 15.3M&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 241
- Cisco IOS Documentation Set, page 241


## 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 15.3M&T releases, see the following URL:

http://www.cisco.com/en/US/products/ps12745/tsd_products_support_series_home.html

# 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, lhash, 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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 241.