



# Release Notes for Cisco 3800 Series Integrated Services Routers with Cisco IOS Release 12.3(11)YZ

---

**August 10, 2007**  
**Last Updated: September 24, 2008**  
**Cisco IOS Release 12.3(11)YZ2**  
**OL-11404-02 Third Release**

These release notes for the Cisco 3800 Series Integrated Services Routers describe the enhancements provided in Cisco IOS Release 12.3(11)YZ. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(11)YZ, see the [Caveats for Cisco IOS Release 12.3 T](#). The caveats document is updated for every maintenance release and is located on [Cisco.com](#).

Use these release notes with [Cross-Platform Release Notes for Cisco IOS Release 12.3 T](#) located on [Cisco.com](#).

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at [http://www.cisco.com/warp/customer/tech\\_tips/index/fn.html](http://www.cisco.com/warp/customer/tech_tips/index/fn.html). If you do not have a Cisco.com login account, you can find field notices at [http://www.cisco.com/warp/public/tech\\_tips/index/fn.html](http://www.cisco.com/warp/public/tech_tips/index/fn.html).

## Contents

These release notes describe the following topics:

- [Inheritance Information, page 2](#)
- [System Requirements, page 3](#)
- [New and Changed Information, page 6](#)
- [Limitations and Restrictions, page 7](#)
- [Caveats for Cisco IOS Release 12.3\(11\)YZ, page 7](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

# Inheritance Information

Cisco IOS Release 12.3(11)YZ are based on Cisco IOS Release 12.3(11)T. All features in Cisco IOS Release 12.3(11)T are in Cisco IOS Release 12.3(11)YZ.

Table 1 lists sections of the *Cross-Platform Release Notes for Cisco IOS Release 12.3 T* that apply to Cisco IOS Release 12.3(11)YZ.

**Table 1** *References for the Cross-Platform Release Notes for Cisco IOS Release 12.3 T*

Topic	Location
<ul style="list-style-type: none"> <li>Introductory information about the Cisco Cisco 3800 Series Integrated Services Routers</li> <li>Hardware Supported</li> <li>Feature Set Tables</li> <li>Additional Notes for the Cisco 3800 Series Integrated Services Routers</li> </ul>	<p>On <a href="http://www.cisco.com">Cisco.com</a> at the following URL:</p> <p><b>Products &amp; Solutions: Cisco IOS Software: All Cisco IOS Software: Cisco IOS Software Releases 12.3 T: Technical Documentation: Release Notes: Cross-Platform Release Notes for Cisco IOS Release 12.3 T, Part 2: Platform-Specific Information</b></p> <p>Or at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123t/123treqs.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123t/123treqs.htm</a></p>
<ul style="list-style-type: none"> <li>Determining the Software Version</li> <li>Upgrading to a New Software Release</li> </ul>	<p>On <a href="http://www.cisco.com">Cisco.com</a> at the following URL:</p> <p><b>Products &amp; Solutions: Cisco IOS Software: All Cisco IOS Software: Cisco IOS Software Releases 12.3 T: Technical Documentation: Release Notes: Cross-Platform Release Notes for Cisco IOS Release 12.2 T, Part 1: System Requirements</b></p> <p>Or at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123/123reqs.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123/123reqs.htm</a></p>
<ul style="list-style-type: none"> <li>Feature Descriptions (New and Changed Information)</li> <li>MIBs</li> <li>Important Notes</li> </ul>	<p>On <a href="http://www.cisco.com">Cisco.com</a> at the following URL:</p> <p><b>Products &amp; Solutions: Cisco IOS Software: All Cisco IOS Software: Cisco IOS Software Releases 12.3 T: Technical Documentation: Release Notes: Cross-Platform Release Notes for Cisco IOS Release 12.3 T, Part 3: New Features and Important Notes</b></p> <p>Or at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123/123newf.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123/123newf.htm</a></p>
<ul style="list-style-type: none"> <li>Related Documentation</li> <li>Obtaining Documentation</li> <li>Obtaining Technical Assistance</li> </ul>	<p>On <a href="http://www.cisco.com">Cisco.com</a> at the following URL:</p> <p><b>Products &amp; Solutions: Cisco IOS Software: All Cisco IOS Software: Cisco IOS Software Releases 12.3 T: Technical Documentation: Release Notes: Cross-Platform Release Notes for Cisco IOS Release 12.3 T, Part 4: Related Documentation</b></p> <p>Or at the following URL:</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123/123docs.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123/123docs.htm</a></p>

- For information on the Cisco 3800 Series Integrated Services Routers, see the following documentation index:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_mod/3800/](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/3800/)

- For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.3(11)YZ, see the “[New and Changed Information](#)” section on page 6.

## System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(11)YZ and includes the following sections:

- [Memory Recommendations](#), page 3
- [Supported Hardware](#), page 4
- [Supported Software](#), page 4
- [Determining the Software Version](#), page 5
- [Upgrading to a New Software Release](#), page 5
- [Feature Set Tables](#), page 6

## Memory Recommendations

[Table 2](#) displays the memory recommendations of the Cisco IOS feature sets for the Cisco Cisco 3800 Series Integrated Services Routers for Cisco IOS Release 12.3(11)YZ.

**Table 2** *Memory Recommendations for the Cisco Cisco 3800 Series Integrated Services Routers*

<b>Platforms</b>	<b>Feature Sets</b>	<b>Software Image</b>	<b>Flash Memory Recommended</b>	<b>DRAM Memory Recommended</b>	<b>Runs From</b>
<b>Cisco 3825, Cisco 3845</b>	Cisco 3825 IOS ENTERPRISE SERVICES	c3825-entservicesk9-mz	64 MB	256 MB	RAM
	Cisco 3825 IOS SPSK9-ESK9 FEAT SET FACTORY UPG FOR BUNDLES	c3825-ipvoice-mz	64 MB	256 MB	RAM
	Cisco 3845 IOS ADVANCED ENTERPRISE SERVICES	c3845-adventerprisek9-mz	64 MB	256 MB	RAM
	Cisco 3845 IOS AISK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES				
	Cisco 3845 IOS ASK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES				
	Cisco 3845 IOS SPSK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES				
	Cisco 3845 IOS ENTERPRISE SERVICES	c3845-entservicesk9-mz	64 MB	256 MB	RAM
Cisco 3845 IOS SPSK9-ESK9 FEAT SET FACTORY UPG FOR BUNDLES					
Cisco 3825 IOS IP VOICE	c3845-ipvoice-mz	64 MB	256 MB	RAM	

## Supported Hardware

For supported hardware information, see the following documentation on Cisco.com:

- [Cisco 3800 Series Hardware Installation](#)
- [Cisco 3800 Series Cards and Modules](#)

## Supported Software

For detailed descriptions of the new software features, see the “[New and Changed Information](#)” section on page 6.

For additional information about supported hardware and software for this platform and release, see the [Hardware/Software Compatibility Matrix](#) in the Cisco Software Advisor at the following location:

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hswsmatrix.cgi>

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 3800 router, log in to the router and enter the **show version EXEC** command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.3(11)YZ Software (c2691-adventerprisek9-mz), Version 12.3(11)YZ1, EARLY
DEPLOYMENT RELEASE SOFTWARE
```

## Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, refer to [How to Choose a Cisco IOS Software Release](#) at the following link:

[http://www.cisco.com/warp/public/130/choosing\\_ios.shtml](http://www.cisco.com/warp/public/130/choosing_ios.shtml)

For information about upgrading to a new software release, refer to the document at the following link:

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

For [Cisco IOS Upgrade Ordering Instructions](#), refer to the following link:

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

To access Cisco Feature Navigator, 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](mailto: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 the following URL:

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

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/jsp/index.jsp>

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

## Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.3(11)YZ supports the same feature sets as Cisco IOS Release 12.3(11)YZ, but Cisco IOS Release 12.3(11)YZ can include new features supported by the Cisco Cisco 3800 Series Integrated Services Routers.

**Caution**

Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States 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 United States government regulations. When applicable, purchaser and 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](mailto:export@cisco.com).

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

<http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml>

**Note**

These release notes are not cumulative and list only features that are new to Cisco IOS Release 12.3(11)YZ. The parent release for Cisco IOS Release 12.3(11)YZ is Cisco IOS Release 12.3(11)T. For information about inherited features, refer to Cisco.com or Cisco Feature Navigator. For Cisco.com, either go to [Cisco.com](http://www.cisco.com) and select the appropriate software release under **Products and Service** and **IOS Software** or go to <http://www.cisco.com/univercd/home/index.htm> and select the appropriate software release under **Cisco IOS Software** and **Release Notes**. If you have a Cisco.com login account, you can use the Cisco Feature Navigator tool at <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>.

## New and Changed Information

### New Hardware and Software Features in Cisco IOS Release 12.4(11)XJ1

There are no new hardware or software features in this release.

### New Software Features in Release 12.3(11)T

For information regarding the features supported in Cisco IOS Release 12.3(11)T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on [Cisco.com](http://www.cisco.com):

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123/index.htm>

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](http://www.cisco.com), and click the following path:

Service & Support: Technical Documents: Cisco IOS Software: Release 12.3: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.3(11)T)

## Limitations and Restrictions

There are no known limitations or restrictions in this release.

## Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

<http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml>

## Field Notices and Bulletins

For general information about the types of documents listed in this section, refer to the following document:

- **Field Notices**—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. Field notices can be found at [http://www.cisco.com/en/US/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html).
- **Product Bulletins**—If you have an account on Cisco.com, you can find product bulletins at <http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml>. If you do not have a Cisco.com login account, you can find product bulletins at <http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml>.
- *What's Hot in Software Center*—Provides information about caveats that are related to deferred software images for Cisco IOS software releases. If you have an account on Cisco.com, you can access the software center at <http://www.cisco.com/kobayashi/sw-center> or by logging in and selecting **Technical Support: Software Center: Cisco IOS Software: What's Hot in Software Center**.
- *What's New in the Software Center*—Recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. You can access **What's New for IOS** by logging into [Cisco.com](http://www.cisco.com) and selecting **Technical Support: Software Center: Products and Downloads: Cisco IOS Software**.

## Caveats for Cisco IOS Release 12.3(11)YZ

Caveats describe unexpected behavior or defects in the Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.



### 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](http://www.cisco.com) and click **Products and Services: Cisco IOS Software: Cisco IOS Software Releases 12.3: Troubleshooting: Bug Toolkit**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

## Resolved Caveats for Cisco IOS Release 12.3(11)YZ2

CSCsd95616

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml>.

CSCse56501

**Symptom** A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

**Workaround** Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>.

CSCsi01470

**Symptom** A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

**Workaround** Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>.

CSCse68138 Issue in handling specific packets in VOIP RTP Lib

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

Session Initiation Protocol (SIP)

Media Gateway Control Protocol (MGCP)

Signaling protocols H.323, H.254

Real-time Transport Protocol (RTP)

Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

CSCsi64851 %DATACORRUPTION-1-DATAINCONSISTENCY unterminated string in buffer

**Symptom** Traceback is seen while configuring “incoming port” using a string [large value 238 characters] for “call filter match-list 1 voice”. Trace shows unterminated string in buffer.

**Conditions** Trace back is seen on executing “show log” after configuring “incoming port” using string of for “call filter match-list 1 voice”.

**Workaround** There is no workaround.

CSCsi74508 data inconsistency error in red\_nvgen\_params

**Symptom** A Cisco IOS device may produce the following error when reading or writing the configuration:

%DATACORRUPTION-1-DATAINCONSISTENCY: write of 11 bytes to 10 bytes

**Conditions** This symptom has been observed when reading or writing the configuration.

**Workaround** There is no workaround.

CSCsi78118 Traceback seen at iphc\_decompress.

**Symptom** A traceback may be generated at the “iphc\_decompress” function.

**Conditions** This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.13)T1 and that is configured for Internet Protocol Header Compression (IPHC). However, note that the symptom is not release-specific.

**Workaround** There is no workaround.

CSCsi78162 SNASw %DATACORRUPTION-1-DATAINCONSISTENCY messages

**Symptom** A router that has the SNASwitch feature enabled may generate several of the following messages along with tracebacks [%DATACORRUPTION-1-DATAINCONSISTENCY](#); copy of xx bytes should be xx bytes

**Conditions** This symptom is observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCsh87705. A list of the affected releases can be found at <http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh87705>. Cisco IOS software releases that are not listed in the “First Fixe-in Version” field at this location are not affected.

**Workaround:** There is no workaround.

**Further Problem Description:** The messages do not affect the normal operation of the router in any way. The SNASwitch continues to function normally.

CSCsj06951 Traceback @ createCNF\_file while configuring user-locale

**Symptom** Traceback seen on terminal.

**Conditions** When config user-locale and generate CNF file under telephony-service.

**Workaround** There is no workaround.

CSCei52653 cipSecTunInOctets/cipSecTunOutOctets report zero  
cipSecTunInOctets/cipSecTunOutOctets is report zero when using c1841-advsecurityk9-mz.123-14.T2.bin.

CSCse05642 I/O memory corruption crash on as5850

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

Session Initiation Protocol (SIP)

Media Gateway Control Protocol (MGCP)

Signaling protocols H.323, H.254

Real-time Transport Protocol (RTP)

Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

CSCsj16292 DATACORRUPTION-1-DATAINCONSISTENCY: copy error

**Symptom** Following an upgrade to Cisco IOS Release 12.2(18)SXF9, the following message may be displayed:

[%DATACORRUPTION-1-DATAINCONSISTENCY](#): copy error

-Traceback=

**Conditions** This message may appear as a result of SNMP polling of PAgP variables, but does not appear to be service impacting.

**Workaround** There is no workaround.

CSCsb79076 MGCP RSVP enabled calls fails due to spurious error @ qosmodule\_main %SYS-3-TIMERNEG errors and tracebacks are observed while making MGCP RSVP calls on a analog (RGW) setups.

**Symptom** Observed in 12.4(3.9)T1 IOS version.

**Workaround** There is no workaround.

CSCsj18014 Caller ID string received with extra characters CSCsf28840 dwind Crash due to configured peer type control vector

**Symptom** A caller ID may be received with extra characters.

**Conditions** This symptom is observed when caller ID is enabled on both routers and when the station ID and station name are configured on the FXS side.

**Workaround** There is no workaround.

CSCsg16908 IOS FTP Server Deprecation

Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the IOS FTP Client feature. This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml>.

CSCin95836 NHRP does not handle error conditions gracefully

The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS?? contains a vulnerability that can result in a restart of the device or possible remote code execution.

NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml>.

CSCsf08998 MGCP stop responding after receiving malformed packet

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

Session Initiation Protocol (SIP)

Media Gateway Control Protocol (MGCP)

Signaling protocols H.323, H.254

Real-time Transport Protocol (RTP)

Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

CSCsg03449 Etherswitch module VLAN Trunking Protocol Vulnerabilities

#### Symptom

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

**Conditions** The packets must be received on a trunk enabled port.

**Further Information:** On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- [CSCsd52629/CSCsd34759](#) -- VTP version field DoS
- [CSCse40078/CSCse47765](#) -- Integer Wrap in VTP revision

- [CSCsd34855/CSCei54611](#) -- Buffer Overflow in VTP VLAN name
- [CSCsg03449](#) -- Etherswitch module VLAN Trunking Protocol Vulnerabilities. Cisco's statement and further information are available on the Cisco public website at: <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

CSCsh58082 SIP: A router may reload due to SIP traffic

Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP. There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workarounds exist to mitigate the effects of this problem on devices which do not require SIP. This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>.

CSCse68355 Router crashed by malformed SIP packet

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

Session Initiation Protocol (SIP)

Media Gateway Control Protocol (MGCP)

Signaling protocols H.323, H.254

Real-time Transport Protocol (RTP)

Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

CSCsc64976 rbisarya HTTP server should scrub embedded HTML tags from cmd output

A vulnerability exists in the IOS HTTP server in which HTML code inserted

into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml>

CSCek26492 Enhancements to Packet Input Path.

**Symptom** A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

**Conditions** This Bug resolves a symptom of CSCec71950. Cisco IOS with this specific Bug are not at risk of crash if CSCec71950 has been resolved in the software.

**Workaround** Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

CSCsg70474 IOS FW with h323 inspect crashes when malformed H.323 packets received  
Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

Session Initiation Protocol (SIP)

Media Gateway Control Protocol (MGCP)

Signaling protocols H.323, H.254

Real-time Transport Protocol (RTP)

Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself. This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

CSCse05736 A router running RCP can be reloaded with a specific packet

**Symptom** A router that is running RCP can be reloaded by a specific packet.

**Conditions** This symptom is seen under the following conditions: - The router must have RCP enabled.  
- The packet must come from the source address of the designated system configured to send RCP packets to the router. - The packet must have a specific data content.

**Workaround** Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

CSCef77013 Tighter parameter checking for ipv6

Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected IOS and IOS XR devices, and may also result in a crash of the affected IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml>

CSCsd81407 Router crash on receiving abnormal MGCP messages

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

Session Initiation Protocol (SIP)

Media Gateway Control Protocol (MGCP)

Signaling protocols H.323, H.254

Real-time Transport Protocol (RTP)

Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself. This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

CSCec12299 Corruption of ext communities when receiving over ipv4 EBGP session

**Symptom** EIGRP-specific Extended Community 0x8800 is corrupted and shown as 0x0:0:0.

**Conditions** This symptom is observed when EIGRP-specific Extended Community 0x8800 is received via an IPv4 EBGP session on a CE router. This occurs typically in the following inter-autonomous system scenario:

**ASBR/PE-1 <----> VRF-to-VRF <----> ASBR/PE-2**

**Workaround** Use a configuration such as the following to remove extended communities from the CE router:

```
router bgp 1
  address-family ipv4 vrf one
  neighbor 1.0.0.1 remote-as 100
  neighbor 1.0.0.1 activate
  neighbor 1.0.0.1 route-map FILTER in
  exit-address-family
!
```

```

ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
  set extcomm-list 100 delete
!

```

CSCsd85587 7200 Router crashes with ISAKMP Codenomicon test suite

A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

The vulnerable cryptographic library is used in the following Cisco products:

- Cisco IOS, documented as Cisco bug ID CSCsd85587
- Cisco IOS XR, documented as Cisco bug ID CSCsg41084
- Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
- Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
- Cisco Firewall Service Module (FWSM) CSCsi97695

This vulnerability is also being tracked by CERT/CC as VU#754281.

Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml> .



**Note**

Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml> and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>

CSCsi60004 H323 Proxy Unregistration from Gatekeeper

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

Session Initiation Protocol (SIP)

Media Gateway Control Protocol (MGCP)

Signaling protocols H.323, H.254

Real-time Transport Protocol (RTP)

Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself. This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

CSCse24889 Malformed SSH version 2 packets may cause processor memory depletion

**Symptom** Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

**Conditions** This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

**Workaround** As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t
ip ssh version 1 end
```

**Alternate Workaround:** Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied

access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any
line vty 0 4
access-class 99 in

end
```

**Further Problem Description:** For information about configuring vty access lists, see the *Controlling Access to a Virtual Terminal Line* document:

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document: <http://www.cisco.com/warp/public/707/ssh.shtml>

CSCse85200 Inadequate validation of TLVs in cdp

**Symptom** Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

**Conditions** Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

**Workaround** Disable interfaces where CDP is not necessary.

CSCsg40567 Memory leak found with malformed tls/ssl packets in http core process

**Symptom** Malformed SSL packets may cause a router to leak multiple memory blocks.

**Conditions** This symptom is observed on a Cisco router that has the ip http secure server command enabled.

**Workaround** Disable the ip http secure server command.

CSCsb12598 Router forced crash on receiving fragmented TLS ClientHello

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>



**Note** Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

CSCsb40304 Router crash on sending repetitive SSL ChangeCipherSpec

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities. This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>




---

**Note** Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:  
<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>

---

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

CSCsd92405 Router crashed by repeated SSL connection with malformed finished message

Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>



**Note** Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:  
<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: <http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

CSCsg96319 reverse ssh eliminated telnet authentication on VTY

**Symptom** When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the  
**ssh -l userid :number ip-address** command.

**Conditions** This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

[http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t11/feature/guide/gt\\_rssh.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_rssh.html)

**Workaround** Configure reverse SSH by entering the **ip ssh port portnum rotary group** command. This configuration is explained at the following URL:

[http://www.cisco.com/en/US/tech/tk583/tk617/technologies\\_q\\_and\\_a\\_item09186a0080267e0f.shtml#ewq1](http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#ewq1)

CSCsj66369 Traceback seen at rpmxf\_dg\_db\_init

**Symptom** Tracebacks seen while running metal\_vpn\_cases.itcl script

**Conditions** A strcpy in the file 'rpmxf\_dg\_online.c' copies more bytes than the destination buffer size. Due to this we are getting data corruption tracebacks.

**Workaround** There is no workaround.

CSCsj66513 Traceback detected at DNQueuePeers

**Symptom** Traceback found at DNQueuePeers

**Conditions** While verifying the variable digit length dialing numbers for “Type National” and “Type International” in the numbering plan to be accepted by the network-side by using  
**functionality/isdn/isdn\_dialPlan** script.

**Workaround** There is no workaround

CSCsj44099 Router crashes if DSPFARM profile description is 128 characters long.

**Symptom** A cisco c3800 router can experience a memory corruption resulting in a crash if the description field under the “dspfarm profile” configuration matches the maximum of 128 characters.

**Conditions** During configuration of the dspfarm profile through the CLI, a description that is 128 characters will cause a memory copy problem. If the user tries to display the results of the configuration using “show dspfarm profile”, the router will crash trying to display the output.

**Workaround** To prevent this problem configure the dspfarm profile description with 127 characters or less.

CSCsj52927 DATACORRUPTION-1-DATAINCONSISTENCY message in show log

**Symptom** DATACORRUPTION-1-DATAINCONSISTENCY messages are seen in ‘show log’.

**Conditions** The messages are seen when when the router comes up.

**Workaround** There is no workaround.

CSCdz55178 QoS profile name of more then 32 chars will crash the router

**Symptom** A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

**Conditions** This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

cable qos profile 12 name g711@10ms\_for\_any\_softswitch\_Traa^C

```
000000001111111111222222222333^
```

```
12345678901234567890123456789012|
```

```
|
```

PROBLEM

(Variable Overflowed).

**Workaround** Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- CSCsf04754

Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml>

## Resolved Caveats for Cisco IOS Release 12.3(11)YZ1

- CSCek37177: The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers.

Workaround: There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>

- CSCsd40334: Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

Cisco has made free software available to address this vulnerability for affected customers.

Workaround: There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml>

- CSCsd58381: Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

Cisco has made free software available to address this vulnerability for affected customers.

Workaround: There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml>

- CSCsb93407: voice-h323 ealyon H323 port tcp 1720 still listening after call service stop

Symptoms: With H323 call service stopped, the router still listens on tcp port 1720 and completes connection attempts.

Conditions: After H323 is disabled using the configuration commands:

```
voice service voip
h323
call service stop
```

Workaround: Access can be blocked by deploying an interface access list that blocks access to TCP port 1720 for traffic that is destined for any of the IP addresses of the router.

For information about deploying access lists, see the "Transit Access Control Lists: Filtering at Your Edge" document:

<http://www.cisco.com/warp/public/707/tacl.html>

For further information about deploying access lists, see the "Protecting Your Core: Infrastructure Protection Access Control Lists" document:

<http://www.cisco.com/warp/public/707/iacl.html>

For information about using control plane policing to block access to TCP port 1720, see the "Deploying Control Plane Policing White Paper:"

[http://www.cisco.com/en/US/products/ps6642/products\\_white\\_paper0900aecd804fa16a.shtml](http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml)

- CSCsc72722: ios-firewall ealyon CBAC - firewall resets TCP idle timer upon receiving invalid TCP packets

Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

Workaround: There is no workaround.

- CSCsb11849: security ealyon CoPP: Need support for malformed IP options

Symptoms: CoPP policy configured to drop packets with IP options will ignore packets with malformed IP options

Conditions: CoPP configured to filter ip packets with IP options

Workaround: Do not use IP option ACL filtering with CoPP. Instead configure CoPP to filter ip packets by source or destination address.

- CSCsb52717: mcast-vpn ealyon Watchdog timeout and crash caused by invalid MDT data group join packet

Symptoms: A Cisco router configured for multicast VPN may reload after receiving a malformed MDT data group join packet.

Conditions: Affects all Cisco IOS versions that support mVPN MDT.

Workaround: Filter out MDT Data Join messages from the router sending the malformed packet using a Receive Access Control List (rACL) feature. Note by doing this, the offending router will not be able to participate within the mVPN data trees.

The following example shows how to block malformed MDT Data Join messages that are sent from the device's IP addresses using a receive ACL:

```
!
ip receive access-list 111
!
access-list 111 deny udp host <ip address of router sending malformed join
request> host 224.0.0.13 eq 3232
access-list 111 permit ip any any
!
```

**Note**

Ensure that the rACL does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering necessary traffic could result in an inability to remotely access the router, thus requiring a console connection. For this reason, lab configurations should mimic the actual deployment as closely as possible. Cisco recommends that you test this feature in the lab prior to deployment. For more information on rACLs, refer to "Protecting Your Core: Infrastructure Protection Access Control Lists" at the following URL:  
<http://www.cisco.com/warp/public/707/racl.html>.

- CSCsd28634: tcl-bleeding ealyon AAA command authorization can be bypassed via TCL scripts from ESS/ESM

Symptoms: Add functionality to disable ESM filter to execute Cisco IOS configuration commands. To prevent configuration commands being executed via ESM TCL filters, enter the global configuration command: **no loggin esm config**

Conditions: Prevents execution of the tcl script command ios\_config from ESM filters.

Further Problem Description: As Tcl script modules contain executable commands, you should manage the security of these files in the same way you manage configuration files."

Workaround: Syslog filter modules can be written and stored as plain-text files or as precompiled files. Tcl script pre-compiling can be done with tools such as TclPro. Precompiled scripts allow a measure of security and managed consistency because they cannot be edited.

- CSCsd92600: pki michaelr RSA keypair is renamed after reload causing Certificate usage to fail

Symptoms: After a reload, the router is unable to use its certificate to establish a VPN connection. If the peer is also a Cisco IOS router, debug crypto isakmp will show the following error during the negotiation:

```
ISAKMP(...): signature invalid!
```

Conditions: Certificate based authentication is used in ISAKMP

Workaround: Re-enroll the router after the reload, to get a new certificate.

Further Problem Description: After the reload, show crypto key mypubkey rsa shows that the RSA keypair used is an old one (the one that was in use before the most recent enrollment) so it does not match the keypair that was used to obtain the current certificate.

The RSA keypair that should be used (the one that was used to obtain the current certificate) has been renamed with a # at the end. For example, before the reload, the rsa keypair is named router.domain.priv. After the reload, this key is now named router.domain.priv#, and there is another (older) keypair named router.domain.priv that does not match the certificate.

## Related Documentation

- [Release-Specific Documents, page 25](#)
- [Platform-Specific Documents, page 25](#)
- [Cisco Feature Navigator, page 26](#)
- [Cisco IOS Software Documentation Set, page 26](#)
- [Cisco.com, page 29](#)
- [Ordering Documentation, page 29](#)

- [Cisco TAC Website, page 30](#)
- [Opening a TAC Case, page 30](#)
- [TAC Case Priority Definitions, page 31](#)

## Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on [Cisco.com](#) and <http://www.cisco.com/univercd/home/index.htm>:

- [Cross-Platform Release Notes for Cisco IOS Release 12.3\(11\)T](#)

On [Cisco.com](#) at:

**Products and Solutions: Cisco IOS Software: Cisco IOS Software Releases 12.3: Instructions and Guides: Release Notes**

On <http://www.cisco.com/univercd/home/index.htm> at:

**Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes**

Cross-Platform Release Notes for Cisco IOS Release 12.3 T are located on [Cisco.com](#) at or on <http://www.cisco.com/univercd/home/index.htm> at **Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cisco IOS Release 12.3 T**.

- Product bulletins, field notices, and other release-specific documents at <http://www.cisco.com/univercd/home/index.htm>
- [Caveats for Cisco IOS Release 12.3](#)

As a supplement to the caveats listed in these release notes, see [Caveats for Cisco IOS Release 12.3](#) and [Caveats for Cisco IOS Release 12.3 T](#), which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T.

On [Cisco.com](#) at:

**Products & Services: IOS Software: Cisco IOS Software Releases 12.3: Instructions and Guides: Release Notes: Release Notes for Cisco IOS Release 12.3, Part 5: Caveats**

On <http://www.cisco.com/univercd/home/index.htm> at:

**Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Caveats**

- 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 click **Products and Solutions: Cisco IOS Software: Cisco IOS Software Releases 12.3: Troubleshooting: Bug Toolkit**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

## Platform-Specific Documents

- [Cisco 3800 Series Cards and Modules](#)
- [Cisco 3800 Series Hardware Installation](#)
- [Cisco 3800 Series Integrated Services Routers](#)

## Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly 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.

To access Cisco Feature Navigator, you must have an account on [Cisco.com](http://Cisco.com). If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with [Cisco.com](http://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](http://Cisco.com) by following the directions found at this URL:

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

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/jsp/index.jsp>

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

### Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On [Cisco.com](http://Cisco.com) at:

**Products and Solutions: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides**

On <http://www.cisco.com/univercd/home/index.htm> at:

**Cisco IOS Software: Cisco IOS Release 12.3: Configuration Guides and Command References**

### Cisco IOS Release 12.3 Documentation Set Contents

**Table 3** lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.

On [Cisco.com](http://Cisco.com) at:

**Products and Solutions: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides**

On <http://www.cisco.com/univercd/home/index.htm> at:

**Cisco IOS Software: Cisco IOS Release 12.3**

**Table 3 Cisco IOS Release 12.3 Documentation Set**

<b>Books</b>	<b>Major Topics</b>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i></li> <li>• <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i></li> </ul>	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2: Bridging</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2: IBM Networking</i></li> </ul>	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Technologies Configuration Guide</i></li> <li>• <i>Cisco IOS Dial Technologies Command Reference</i></li> </ul>	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface and Hardware Component Configuration Guide</i></li> <li>• <i>Cisco IOS Interface and Hardware Component Command Reference</i></li> </ul>	LAN Interfaces Serial Interfaces Logical Interfaces

**Table 3 Cisco IOS Release 12.3 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Configuration Guide</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility</i></li> </ul>	<ul style="list-style-type: none"> <li>IP Addressing and Services</li> <li>IP Routing Protocols</li> <li>IP Multicast</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>AppleTalk</li> <li>Novell IPX</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Apollo Domain</li> <li>Banyan VINES</li> <li>DECnet</li> <li>ISO CLNS</li> <li>XNS</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice Configuration Library</i></li> <li>• <i>Cisco IOS Voice Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Voice over IP</li> <li>Call Control Signaling</li> <li>Voice over Frame Relay</li> <li>Voice over ATM</li> <li>Telephony Applications</li> <li>Trunk Management</li> <li>Fax, Video, and Modem Support</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Packet Classification</li> <li>Congestion Management</li> <li>Congestion Avoidance</li> <li>Policing and Shaping</li> <li>Signaling</li> <li>Link Efficiency Mechanisms</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide</i></li> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>AAA Security Services</li> <li>Security Server Protocols</li> <li>Traffic Filtering and Firewalls</li> <li>IP Security and Encryption</li> <li>Passwords and Privileges</li> <li>Neighbor Router Authentication</li> <li>IP Security Options</li> <li>Supported AV Pairs</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Cisco IOS Switching Paths</li> <li>NetFlow Switching</li> <li>Multiprotocol Label Switching</li> <li>Multilayer Switching</li> <li>Multicast Distributed Switching</li> <li>Virtual LANs</li> <li>LAN Emulation</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>ATM</li> <li>Broadband Access</li> <li>Frame Relay</li> <li>SMDS</li> <li>X.25 and LAPB</li> </ul>

**Table 3** Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Mobile Wireless Configuration Guide</i></li> <li>• <i>Cisco IOS Mobile Wireless Command Reference</i></li> </ul>	General Packet Radio Service
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Terminal Services Configuration Guide</i></li> <li>• <i>Cisco IOS Terminal Services Command Reference</i></li> </ul>	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Software System Messages</i></li> </ul>	

## Obtaining Documentation

Cisco documentation and additional literature are available on [Cisco.com](http://www.cisco.com). Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/cisco/web/support/index.html>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered [Cisco.com](http://www.cisco.com) users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered [Cisco.com](http://Cisco.com) users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit e-mail comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems

Attn: Customer Document Ordering

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. [Cisco.com](http://Cisco.com) features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

## Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a [Cisco.com](http://Cisco.com) user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

## Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

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

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives.

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private Internets and Intranets. You can access the Internet Protocol Journal at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

Use this document in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007, Cisco Systems, Inc. All rights reserved.

