



# Release Notes for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 Universal Gateways with Cisco IOS Release 12.3(11)YZ

---

March 26, 2008  
Cisco IOS Release 12.3(11)YZ2  
OL-11418-02 Initial Release

These release notes describe new features and significant software components for the Cisco 5x00 Universal Gateways that support Cisco IOS Release 12.3(11)YZ. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the [Cross-Platform Release Notes for Cisco IOS Release 12.3T](#).

For a list of the software caveats that apply to Release 12.3(11)YZ, see the [“Caveats for Cisco IOS Release 12.3\(11\)YZ” section on page 5](#) and [Caveats for Cisco IOS Release 12.3\(11\)T](#). The online caveats document is updated for every maintenance release.

## Contents

- [System Requirements, page 1](#)
- [New and Changed Information, page 3](#)
- [Limitations and Restrictions, page 4](#)
- [Caveats for Cisco IOS Release 12.3\(11\)YZ, page 5](#)
- [Related Documentation, page 21](#)

## System Requirements

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



---

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

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Caveats for Cisco IOS Release 12.3\(11\)YZ, page 5](#)

## Memory Requirements

[Table 1](#), [Table 2](#), and [Table 3](#) describe the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Cisco IOS Release 12.3(11)YZ on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 universal gateways.

**Table 1** *Memory Requirements for the Cisco AS5350 Universal Gateway*

Feature Set	Software Image	Flash Memory	DRAM
IP PLUS IPSEC 56	c5350-ik8s-mz	32	128
IP Plus	c5350-is-mz	32	128
IP Plus IPsec 3DES	c5350-ik9s-mz	32	128
IP Plus IPsec 3DES Lawful Intercept	c5350-ik9su2-mz	64	256
Enterprise Plus	c5350-js-mz	64	128
ENTERPRISE PLUS IPSEC 56	c5350-jk8s-mz	64	128
Enterprise Plus IPsec 3DES	c5350-jk9s-mz	64	128

**Table 2** *Memory Requirements for the Cisco AS5400 Universal Gateway*

Feature Set	Software Image	Flash Memory	DRAM
IP Plus	c5400-is-mz	64	256
IP Plus IPsec 3DES	c5400-ik9s-mz	64	256
IP Plus IPsec 3DES Lawful Intercept	c5400-ik9su2-mz	64	256
IP PLUS IPSEC 56	c5400-ik8s-mz	64	256
Enterprise Plus	c5400-js-mz	64	256
Enterprise Plus IPsec 3DES	c5400-jk9s-mz	64	256

**Table 3** *Memory Requirements for the Cisco AS5850 Universal Gateway*

Image Name	Software Image	Flash Memory	DRAM Memory
Service Provider Plus	c5850-p9-mz	64 MB	512 MB
Service Provider Plus IPsec 56	c5850-k8p9-mz	64 MB	512 MB
Service Provider Plus IPsec 3DES	c5850-k9p9-mz	64 MB	512 MB

**Table 3**      **Memory Requirements for the Cisco AS5850 Universal Gateway (continued)**

Image Name	Software Image	Flash Memory	DRAM Memory
SP PLUS IPSEC 3DES FOR LAWFUL INTERCEPT	c5850-k9p9u2-mz	64 MB	512 MB
ERSC SERVICE PROVIDER PLUS IPSEC 56	c5850tb-k8p9-mz	64 MB	1024 MB
ERSC SERVICE PROVIDER PLUS IPSEC 3DES	c5850tb-k9p9-mz	64 MB	1024 MB
SP PLUS IPSEC 3DES FOR LAWFUL INTERCEPT	c5850tb-k9p9u2-mz	64 MB	1024 MB
ERSC SERVICE PROVIDER PLUS	c5850tb-p9-mz	64 MB	1024 MB

## Hardware Supported

- Cisco AS5350
- Cisco AS5400
- Cisco AS5400HPX
- Cisco AS5850

## Determining the Software Version

To determine which version of Cisco IOS software is currently running on your Cisco 5x00 universal gateway, log in to the and enter the **show version EXEC** command. The following sample output from the **show version** command indicates the version number.

```
> show version
Cisco Internetwork Operating System Software
IOS (tm) C5x00 Software (C5x00-Y7-MZ), Version 12.4(11)XJ, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.3(11)T
```

## Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to the *Software Installation and Upgrade Procedures* located at <http://www.cisco.com/web/psa/products/index.html>.

## New and Changed Information

### New Hardware and Software Features in Cisco IOS Release 12.3(11)YZ1

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 at:

[http://www.cisco.com/en/US/docs/ios/12\\_3/release/notes/123mcav2.html](http://www.cisco.com/en/US/docs/ios/12_3/release/notes/123mcav2.html)

## 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/en/US/products/products\\_security\\_advisories\\_listing.html](http://www.cisco.com/en/US/products/products_security_advisories_listing.html)

## Field Notices and Bulletins

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

[http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/1654\\_pp.htm](http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/1654_pp.htm)

- **Field Notices**—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)
- **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 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. If you have an account on Cisco.com, you can access *What's New for IOS* at <http://www.cisco.com/cisco/web/download/index.html> or by logging into 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

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>

CSCse56501

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.

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

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.

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-advsecurity9-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.

Symptoms: 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:

[http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec\\_cntrl\\_acc\\_vtl.html](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cntrl_acc_vtl.html)

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#newq1](http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1)

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 than 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
```

```
0000000001111111111222222222333^
```

```
12345678901234567890123456789012l
```

```
|
```

PROBLEM

(Variable Overflowed).

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

## 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-IO-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 22](#)

- [Platform-Specific Documents](#), page 22

## Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3:

- [Cross-Platform Release Notes for Cisco IOS Release 12.3\(11\)T](#)
- 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 AS5350](#)
- [Cisco AS5400](#)
- [Cisco AS5850](#)

## 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.

### 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. *Cisco IOS Software Documentation* is available in html or pdf form.

Select your release and click the command references, configuration guides, or any other Cisco IOS documentation you need.

## Notices

See the “Notices” section in *About Cisco IOS Release Notes* located at:  
[http://www.cisco.com/en/US/docs/ios/12\\_4/12\\_4x/12\\_4xy15/ReleaseNote.html](http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html)

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

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0812R)

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

© 2007-2009, Cisco Systems, Inc. All rights reserved.

