



# Release Notes for the Cisco 800 Series and Cisco SOHO 90 Series Routers with Cisco IOS Release 12.3(8)YG

---

September 24, 2008  
Cisco IOS Release 12.3(8)YG6  
OL-11400-02

These release notes describe new features and significant software components for the Cisco SOHO 90 and Cisco 828 series routers that support Cisco IOS Software Release 12.3(8)YG. 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.

For a list of the software caveats that apply to Cisco IOS Release 12.3(8)YG, see the “[Caveats](#)” section on [page 8](#) and *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* located on [Cisco.com](#).

We recommend you to 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

- [System Requirements, page 2](#)
- [New and Changed Information, page 5](#)
- [Caveats, page 8](#)
- [Additional References, page 28](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 29](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

# System Requirements

This section describes the system requirements for Cisco IOS 12.3(8)YG releases.

## Memory Requirements

Table 1 lists the memory requirements for Cisco IOS 12.3(8)YG.


**Note**

Recommended memory is the memory required for potential future expansions.

**Table 1** *Memory Requirements for the Cisco 800 Series and SOHO Series Routers*

Platform	Image Name	Feature Set	Image	Flash Memory		DRAM Memory	
				Min.	Recom.	Min.	Recom.
Cisco 828	Cisco 828 Series IOS IP/FW PLUS 3DES	IP/FW PLUS 3DES	c828-k9osy6-mz	8 MB	8 MB	32 MB	32 MB
	Cisco 828 Series IOS IP/FW	IP/FW	c828-oy6-mz	8 MB	8 MB	24 MB	24 MB
	Cisco 828 Series IOS IP PLUS	IP PLUS	c828-sy6-mz	8 MB	8 MB	32 MB	32 MB
	Cisco 828 Series IOS IP	IP	c828-y6-mz	8 MB	8 MB	24 MB	24 MB
Cisco 831	Cisco 831 Series IOS IP/FW 3DES	IP/FW 3DES	c831-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 831 Series IOS IP/FW/PLUS 3DES	IP/FW/PLUS 3DES	c831-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
Cisco 836	Cisco 836 Series IOS IP/FW2 IPsec 3DES	IP/FW2/IPsec 3DES	c836-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 836 Series IOS IP/FW2 Plus IPsec 3DES	IP Plus/FW2/IPsec 3DES	c836-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 836 Series IOS IP/FW2/Dial Backup Plus IPsec 3DES	IP Plus/FW2/Dial Backup IPsec 3DES	c836-k9o3s8y6-mz	12 MB	12 MB	48 MB	48 MB
Cisco 837	Cisco 837 Series IOS IP/FW2 IPsec 3DES	IP/FW2/IPsec 3DES	c837-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 837 Series IOS IP/FW2 Plus IPsec 3DES	IP Plus/FW2/IPsec 3DES	c837-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
Cisco SOHO 91	Cisco SOHO 91 Series IOS IP/FW 3DES	IP/FW 3DES	soho91-k9oy6-mz	8 MB	8 MB	32 MB	32 MB
Cisco SOHO 96	Cisco SOHO 96 Series IOS IP/FW/3DES	IP/FW 3DES	soho96-k9oy1-mz	8 MB	8 MB	32 MB	48 MB

**Table 1** Memory Requirements for the Cisco 800 Series and SOHO Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory		DRAM Memory	
				Min.	Recom.	Min.	Recom.
Cisco SOHO 97	Cisco SOHO 97 Series IOS IP/FW	IP/FW	soho97-oy1-mz	8 MB	8 MB	32 MB	32 MB
	Cisco SOHO 97 Series IOS IP/FW/3DES	IP/FW 3DES	soho97-k9oy1-mz	8 MB	8 MB	32 MB	32 MB

## Hardware Supported

The Cisco IOS Release 12.3(8)YG releases support the following routers:

- Cisco 831
- Cisco 836
- Cisco 837
- Cisco SOHO 91
- Cisco SOHO 96
- Cisco SOHO 97

## Determining the Software Version

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

```
Router> show version
```

```
Cisco IOS Software, C837 Software (C837-K903SY6-M),  
Version 12.3(8)YG5, RELEASE SOFTWARE (fc1) Synched to technology version 12.3(8)T  
Technical Support: http://www.cisco.com/techsupport  
(c) 1986-2007 by Cisco Systems, Inc.
```

## Upgrading to a New Software Release

For general information about upgrading to a new software release, see the Software Installation and Upgrade Procedures located at: [http://www.cisco.com/warp/public/130/upgrade\\_index.shtml](http://www.cisco.com/warp/public/130/upgrade_index.shtml).

## Feature Set Tables

Table 2 through Table 7 list the features and feature sets supported in Cisco IOS 12.3(8)YG.

## Feature List by Feature Set for Cisco SOHO Series Routers

**Table 2** Feature List for Feature Set for Cisco SOHO 91 Routers

Feature	In	Feature Set
		IP/FW 3DES
RBE client side encapsulation (without QoS)	12.3(8)YG	-

**Table 3** Feature List for Feature Set for Cisco SOHO 96 Routers

Feature	In	Feature Set
		IP/FW 3DES
RBE client side encapsulation (without QoS)	12.3(8)YG	-

**Table 4** Feature List for Feature Set for Cisco SOHO 97 Routers

Feature	In	Feature Set
		IP/FW 3DES
RBE client side encapsulation (without QoS)	12.3(8)YG	-

## Feature List by Feature Set for Cisco 83X Series Routers

**Table 5** Feature List for Feature Set for Cisco 831 Routers

Feature	In	Feature Set	
		IP/FW 3DES	IP/FW/PLUS
RBE client side encapsulation (with QoS)	12.3(8)YG	Yes	Yes
DMZ Ethernet as backup interface	12.3(8)YG	Yes	Yes

**Table 6** Feature List for Feature Set for Cisco 836 Routers

Feature	In	Feature Set		
		IP/FW 3DES	IP/FW/PLUS	IOS IP/FW/PLUS ISDN DIAL BKUP 3DES VPN
RBE client side encapsulation (with QoS)	12.3(8)YG	Yes	Yes	Yes
DMZ Ethernet as backup interface	12.3(8)YG	Yes	Yes	Yes

**Table 7** Feature List for Feature Set for Cisco 837 Routers

Feature	In	Feature Set	
		IP/FW 3DES	IP/FW/PLUS
RBE client side encapsulation (with QoS)	12.3(8)YG	Yes	Yes
DMZ Ethernet as backup interface	12.3(8)YG	Yes	Yes

## New and Changed Information

This section contains the following new and changed feature information for Cisco IOS Release 12.3(8)YG:

- [New Features in Cisco IOS Release 12.3\(8\)YG6, page 5](#)
- [New Features in Cisco IOS Release 12.3\(8\)YG5, page 5](#)
- [New Features in Cisco IOS Release 12.3\(8\)YG4, page 6](#)
- [New Features in Cisco IOS Release 12.3\(8\)YG3, page 6](#)
- [New Features in Cisco IOS Release 12.3\(8\)YG2, page 6](#)
- [New Features in Cisco IOS Release 12.3\(8\)YG1, page 6](#)
- [New Features in Cisco IOS Release 12.3\(8\)YG, page 7](#)

### New Features in Cisco IOS Release 12.3(8)YG6

#### New Hardware Features

There are no new hardware features in this release.

#### New Software Features

There are no new software features in this release.

### New Features in Cisco IOS Release 12.3(8)YG5

#### New Hardware Features

There are no new hardware features in this release.

#### New Software Features

There are no new software features in this release.

## **New Features in Cisco IOS Release 12.3(8)YG4**

### **New Hardware Features**

There are no new hardware features in this release.

### **New Software Features**

There are no new software features in this release.

## **New Features in Cisco IOS Release 12.3(8)YG3**

### **New Hardware Features**

There are no new hardware features in this release.

### **New Software Features**

There are no new software features in this release.

## **New Features in Cisco IOS Release 12.3(8)YG2**

### **New Hardware Features**

There are no new hardware features in this release.

### **New Software Features**

There are no new software features in this release.

## **New Features in Cisco IOS Release 12.3(8)YG1**

### **New Hardware Features**

There are no new hardware features in this release.

### **New Software Features**

There are no new software features in this release.

# New Features in Cisco IOS Release 12.3(8)YG

## New Hardware Features

There are no hardware features in this release.

## New Software Features

### RBE with QoS

RBE was developed to address known RFC1483 bridging issues, including broadcast storms and security.

Bridging depends heavily on broadcasts in order to establish connectivity. Broadcasts between of users are inherently unscalable since the broadcasts eat up bandwidth across the user's xDSL loop and resources are required at the head-end router to replicate packets for the broadcast over a point-to-point (ATM PVC) media.

From the network point of view, the ATM connection looks like a routed connection with RBE. Data traffic is received as RFC1483 packets, but they are RFC 1483 Ethernet or IEEE 802.3 frames. Instead of bridging the Ethernet or IEEE 802.3 frame, as in the case of regular RFC1483 bridging, the router routes on the Layer 3 header. With the exception of some cursory checks, the bridge header is ignored.

From an operational point of view, the router operates as if the routed-bridge interface were connected to an Ethernet LAN. The operation is described below in two ways: packets originating from the customer premises and packets destined for the customer premises.

For packets originating from the customer premises, the Ethernet header is skipped and the destination IP address is examined. If the destination IP address is in the route cache, the packet is fast-switched to the outbound interface. If the destination IP address is not in the route cache, the packet is queued for process switching. In the process switch mode, the outbound interface through which the packet must be routed is found by looking in the routing table. After the outbound interface is identified, the packet is routed through that interface. This occurs without the requirement for a bridge group or BVI.

For packets destined for the customer premises, the destination IP address of the packet is examined first. The destination interface is determined from the IP routing table. Next, the router checks the Address Resolution Protocol (ARP) table associated with that interface for a destination MAC address to place in the Ethernet header. If none is found, the router generates an ARP request for the destination IP address. The ARP request is forwarded to the destination interface only. This is in contrast to bridging, in which the ARP request is sent to all interfaces in the bridge group or Bridge-Group Virtual Interface (BVI).

RBE was originally known as ATM Half-Bridging.

### DMZ Ethernet as Back Up Interface

The DMZ Ethernet port is supported as a backup interface. This interface supports static addresses, DHCP clients, or PPOE clients. An Ethernet 2 interface can be enabled on the Cisco 830 series routers. Port 4 on the switch is the physical representation of this port.

# Caveats

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. Caveats of all three levels are listed below.


**Note**

If you have an account with [Cisco.com](http://www.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 **Service & Support: Technical Assistance Center: Tool Index: 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 - Cisco IOS Release 12.3\(8\)YG6, page 8](#)
- [Open Caveats - Cisco IOS Release 12.3\(8\)YG6, page 17](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(8\)YG5, page 17](#)
- [Open Caveats - Cisco IOS Release 12.3\(8\)YG4, page 20](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(8\)YG4, page 20](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(8\)YG3, page 21](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(8\)YG2, page 23](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(8\)YG1, page 24](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(8\)YG, page 27](#)

## Resolved Caveats - Cisco IOS Release 12.3(8)YG6

- 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>.
- 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>

- CSCee41508 RSVP red zone crash
 

Symptom: An IOS device may crash when processing a malformed Resource ReSerVation Protocol (RSVP) packet.

Conditions: A device using an affected software version is configured for RSVP and a certain malformed RSVP packet is received.

Workaround: If RSVP is required, no workaround exists. If RSVP is not required, disabling RSVP on all interfaces removes any exposure to this issue. RSVP can be disabled using the `no ip rsvp bandwidth interface` configuration command. The `show ip rsvp EXEC` command can be used on an IOS device to determine if RSVP functionality has been enabled. The `show ip rsvp interface EXEC` command may be used to identify the specific interfaces on which RSVP has been enabled.
- CSCek37177: malformed tcp packets deplete processor memory.
 

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.

This issue is documented as Cisco bug ID CSCek37177

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>
- CSCsb33172: short-circuit crypto engine operations when faking AM2
 

A vulnerability exists in the way some Cisco products handle IKE phase I messages which allows an attacker to discover which group names are configured and valid on the device. A Cisco Security Notice has been published on this issue and can be found at the following URL: <http://www.cisco.com/warp/public/707/cisco-sn-20050624-vpn-grpname.shtml>
- CSCin95836: NHRP does not handle error conditions gracefully
 

Symptoms: A Cisco IOS device configured for NHRP may restart.

Workarounds: There is no workaround.
- CSCsa53334: Bus error in single\_pkt\_regex
 

The Intrusion Prevention System (IPS) feature set of Cisco IOS® contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml>
- CSCsc64976: 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>

- CSCse24889: Malformed SSH version 2 packets may cause processor memory depletion

Symptoms: 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/products/ps6441/products\\_configuration\\_guide\\_chapter09186a0080716ec2.html](http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a0080716ec2.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>

- CSCsc72722: 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.

- **CSCsj18014: Caller ID string received with extra characters**

Symptoms: 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.
- **CSCse85200: Inadequate validation of TLVs in cdp**

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.

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.
- **CSCsf07847: cdp may fail to discover neighbor information in releases wh [CSCse85200](#)**

Symptoms: 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: This issue occurs in IOS images that has the fix for [CSCse85200](#).

Workaround: Disable CDP on interfaces where CDP is not required.

Further Problem Description: Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.
- **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>.
- **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>

- 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>.

- CSCse05736: A router running RCP can be reloaded with a specific packet  
Symptoms: 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.

- CSCsb11849: CoPP: Need support for malformed IP options

Symptom: 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.

- CSCin90682: Unsolicited mode config request packet issue

Symptom: A Cisco IOS device configured for IKE/IPSec may reload.

Conditions: A Cisco IOS device is configured for IKE/IPsec and receives a crafted IKE packet.

Workaround: Disable IPsec.

- CSCsg96319: reverse ssh eliminated telnet authentication on VTY

Symptoms: 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/products/ps6350/products\\_configuration\\_guide\\_chapter09186a00804831b6.html](http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804831b6.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)

- 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>.

- CSCse56501: two sockets(IP V4 and V6) bound to the same UDP port not working.

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>.

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

Symptoms: 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.

- CSCsc72722: 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.

- 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>.

- CSCsj18014: Caller ID string received with extra characters  
Symptoms: 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.
- CSCse85200: Inadequate validation of TLVs in cdp  
Symptoms: 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.  
Condition: 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.
- CSCsj16292: DATACORRUPTION-1-DATAINCONSISTENCY: copy error  
Symptoms: 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.
- 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>.

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

Symptoms: When H323 call service stops, the router still listens on TCP port 1720 and completes connection attempts.

Conditions: This symptom occurs after H323 is disabled using the following 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 at: <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 at: <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” at:

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

- CSCdz55178: QoS profile name of more than 32 chars will crash the router

Symptom: System reloads unexpectedly or other serious side-effects such as memory corruption occur.

Conditions: A cable qos profile with a length greater than 32 characters is configured on the system.

For example:

```

cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                                0000000001111111111222222222333^
                                12345678901234567890123456789012|
                                                                    |
                                                                    PROBLEM (Variable
Overflowned) .
    
```

Workaround: Change the qos profile name to a value less than 32 characters.

Further Problem Description: The variable which holds the value for the string name only allows for 32 characters and the code did not properly truncate names longer than the associated buffer.

This caused other locations in memory to be corrupted.

- 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.

- CSCsj66369: Traceback seen at rpmxf\_dg\_db\_init  
Symptom: Tracebacks seen while running metal\_vpn\_cases.itcl script  
Condition: A strepy 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
- CSCsj52927: DATACORRUPTION-1-DATAINCONSISTENCY message in show log  
Symptom: DATACORRUPTION-1-DATAINCONSISTENCY messages are seen in show log'  
Conditions: The messages are seen when the router comes up.  
Workaround: There is no workaround.

## Open Caveats - Cisco IOS Release 12.3(8)YG6

There are no open caveats in this release.

## Resolved Caveats - Cisco IOS Release 12.3(8)YG5

- CSCsb04965: c2400 devices incorrectly identified as a DOCSIS devices  
A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.  
Workaround: Cisco is 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-20060920-docsis.shtml>.
- CSCsb06658: mwr1900 incorrectly identified as a DOCSIS devices  
A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.  
Workaround: Cisco is 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-20060920-docsis.shtml>.

- CSCsa94162: dhcp ealyon DHCP: Next-hop of static route does not change
 

Symptoms: A DHCP client router has an old static route and a new static route concurrently. The output of the debug dhcp detail on the DHCP client router shows that the old static route is removed but that the routing table still contains the old static route. Also, the old static route is not removed after the static configuration is deleted.

Conditions: This symptom is observed when a DHCP server renews the DHCP address and the DHCP gateway.

Workaround: There is no workaround.
- CSCed09685: Cisco IOS should not send passwords and sensitive information to ACS logs
 

Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

Conditions: This problem happens only with command accounting enabled.

Workaround: Disable command accounting.
- CSCef87827: dhcp ealyon DHCP client route tracking does not remove static dhcp routes
 

Symptoms: IP routes that are inserted by DHCP are not removed from the routing table, and the tracked object goes down.

Conditions: This symptom is observed when you enter the ip dhcp client route track object command. DHCP removes the 0.0.0.0/0 route but not any static routes that use the dhcp keyword for the IP next-hop address, even though DHCP adds both the 0.0.0.0/0 route and these static routes to the routing table.

Workaround: There is no workaround.
- CSCej30903: Enable View Command fails with AAA turned on
 

Symptoms: A router allows logging into the root (or any other configured) view without prompting for a password.

Conditions: This symptom is observed when no method list is configured for login service.

Workaround: Configure a method list for the login service.
- CSCsa43465: None method in default login method list allows enabling with no password
 

Symptom: Users under specified conditions may be able to access privilege level 15 without entering a password.

Conditions: In Cisco IOS versions 12.3(7)T and later, which support Role-Based CLI Access the use of the 'none' method in the default login method list may allow users to enter root view mode (privilege level 15) without entering a password.

For example, if the customer configures:

```
aaa authentication login default group tacacs+ none
```

If the TACACS+ server is down, users are allowed to enter non-privileged mode. However, they can also can enable into root view access through the "enable view" command without having to enter a password.

Workaround: The resolution of the DDTs puts authentication of 'enable view' to the default enable method list. Prior to software upgrade a workaround is too ensure that the method 'none' is not in the default login methods list.

- CSCsb11124: SGBP Crafted Packet Denial of Service

The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability. Cisco has published a Security Advisory on this issue; it is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

- CSCse55588: Router crashes repeatedly at memcpy

Symptoms: Several c836 crashes at least once a day at memcpy with same traceback in YG4

Workaround: There is no workaround.

- CSCeh73049: tcl-bleeding ealyon tclsh mode bypasses aaa command authorization check

Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Conditions: Devices that are not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability. This vulnerability is present in all versions of Cisco IOS that support the tclsh command.

Workaround: This advisory with appropriate workarounds is posted at

<http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml>

- CSCei29471: dhcp ealyon Cannot link static route pointing to DHCP to an interface

Symptoms: Static route specifying both 'interface' and 'DHCP' does not link the DHCP learned Next Hop to an interface, which is not consistent with the non-DHCP variations and confusing to users as it is a departure of what the specified interface means when compared to other "ip route" command variations.

The change is to make DHCP consistent with the non-DHCP cases.

Configuration command:

```
ip route 172.16.1.1 255.255.255.255 FastEthernet0 dhcp
```

From this (in show ip route):

```
172.16.0.0/32 is subnetted, 1 subnets
S      172.16.1.1 [1/0] via 10.1.11.1
```

To this (in show ip route):

```
172.16.0.0/32 is subnetted, 1 subnets
S      172.16.1.1 [1/0] via 10.1.11.1, FastEthernet0
```

Conditions: This occurs when ip route <net> <mask> <interface> dhcp is configured.

Workaround: There is no workaround.

- CSCsb52717: 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. As always, 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:

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

## Open Caveats - Cisco IOS Release 12.3(8)YG4

- CSCeg41935: DDNS - Question mark is not understood by parser  
Symptoms: Unable to configure Dynamic DNS IOS support with HTTP method if URL string contains a question mark. CLI interprets the question mark as a request for context sensitive help.  
Workaround: Use %3F instead of ? when configuring Dynamic DNS IOS support.

## Resolved Caveats - Cisco IOS Release 12.3(8)YG4

- CSCsb31743: Router seeing %SYS-3-INVMEMINT errors  
Symptoms: A Cisco Router may experience the following error messages:  
Jul 4 18:10:06.089: %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level  
-Traceback= 80228B4C 803537AC 8043D254 8043D530 80438840 80340788 8043F89C  
80340710 8034126C 80343EB8 80347C9C Jul 4 18:10:06.089: %SYS-2-MALLOCFAIL:  
Memory allocation of 1024 bytes failed from 0x8043D250, alignment 4 Pool: I/O Free:  
1991832 Cause: Interrupt level allocation Alternate Pool: None Free: 0 Cause: No Alternate  
pool -Process= “<interrupt level>”, ipl= 4 -Traceback= 80228B4C 8034BEFC 80354260  
8043D254 8043D530 80438840 80340788 8043F89C 80340710 8034126C 80343EB8  
80347C9C  
Conditions: The symptom was observed on the Cisco 836 router running IOS release 12.3(11)T3.  
Workaround: There is no workaround.
- CSCef89364: Traceback at Dynamic DNS Update Timer Process  
Symptoms: A Cisco router may show the following line while scrolling down the log:  
Process= “Dynamic DNS Update Timer Process,” ipl= 0, pid= 40 -Traceback= 0x412044F0  
0x4009B7B0 0x412CAC40 0x412CC3BC 0x422B5C2C 0x422B5C10.  
The router needs to be rebooted to recover.

Conditions: This error is observed when removing a **ip ddns update** from an interface, and after entering **shutdown** followed by **no shutdown** on the interface, on a Cisco router running IOS version 12.4(1a).

Workaround: Do not configure the using following sequence:

**shutdown** followed by **no shutdown** after removing **ip ddns update** from the interface.

- CSCsc44237: memory leak in client applications iterating over an empty idb list

This caveat consists of two symptoms, two conditions, and two workarounds:

First symptom: A switch or router that is configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.

The output of the **show processes memory** command shows that the “ATM PA Helper” process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the “Iterator” process holds the memory.

First condition: This symptom is observed on a Cisco switch or router that runs a Cisco IOS software image that contains the fixes for caveats CSCeh04646 and CSCeb30831. A list of the affected releases can be found at:

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh04646> and  
<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeb30831>.

Cisco IOS software releases that are not listed in the “First Fixed-in Version” fields at these locations are not affected.

First workaround: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when you re-insert the PA-A3 ATM port adapter.

Second symptom: A switch or router that has certain PIM configurations may eventually run out of memory.

The output of the **show processes memory** command shows that the “PIM process” does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the “Iterator” process holds the memory.

Second condition: This symptom observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCef50104.

A list of the affected releases can be found at:

<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef50104>.

Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

Second workaround: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf vrf-name** command is configured, enter the **ip vrf forwarding vrf-name** command on at least one interface that has PIM enabled.

## Resolved Caveats - Cisco IOS Release 12.3(8)YG3

- CSCsb24007

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>

- CSCeh60551: certificate crashes 12.3.4.JA AP  
Symptoms: Certain malformed client certificates may cause an AP running 12.3.2.JA2 or 12.3.4.JA to crash when EAP-TLS is used.  
Workaround: Issue a new client certificate.
- CSCei61732: Additional data integrity check in system timer  
Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.  
Cisco has made free software available that includes the additional integrity checks for affected customers.  
This advisory is posted at:  
<http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.
- CSCsa54608: Cisco IOS Firewall Auth-Proxy for FTP/Telnet Sessions buffer overflow  
The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.  
Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.  
Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.  
Only devices running certain versions of Cisco IOS are affected.  
Workaround: Cisco has made free software available to address this vulnerability. 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-20050907-auth\\_proxy.shtml](http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml)
- CSCeh35823: Alpha:free memory reduces in less than half an hour (memory leak)  
Symptoms: When a router detects "invalid identity" failures while decrypting IPsec packets, a memory leak occurs for the packet memory that is associated with these failed packets.  
Conditions: This symptom is observed only when an "invalid identity" error occurs, which is an uncommon error that indicates that the originating router does not send packets according to what was originally negotiated. However, if there is another error that causes a "bad" decryption, the packet could be invalid and may also cause the symptom to occur.

- Workaround: There is no workaround.
- CSCei27330: SYS-2-BADSHARE appears frequently on router log  
Symptoms: A router that is configured for Dynamic Multipoint VPN (DMVPN) may frequently generate the following error message: %SYS-2-BADSHARE: Bad refcount in datagram\_done  
Conditions: This symptom is observed on a Cisco router such as a Cisco 871 and Cisco 1800 series that function as a DMVPN spoke.  
Workaround: There is no workaround.
  - CSCeg15044: Not able to telnet to card (No Free TTY's error).  
Symptoms: Although there are free tty lines, you cannot make a Telnet connection and a "No Free TTYs error" message is generated.  
Conditions: This symptom is observed when there are simultaneous Telnet requests.  
Workaround: "clear tcp tcb" should clear the line.
  - CSCeh13489: BGP shouldn't propagate updates with AS Path lengths greater than 255  
Symptoms: A router may reset its Border Gateway Protocol (BGP) session.  
Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.  
Workaround: Configure the `bgp maxas limit` command in such a way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

## Resolved Caveats - Cisco IOS Release 12.3(8)YG2

- CSCsa61989: L2TPv3 should not allow MTU increase based on ICMP.  
Symptoms: A router running L2TPv3 using Path-MTU Discovery (PMTUD) may incorrectly increase the discovered MTU solely based on information contained in ICMP packet-too-big messages (ICMP 3/4).  
Workaround: There is no workaround.
- CSCsa74819: Cannot disable **vpdn ip udp ignore checksum** across reloads.  
Symptoms: In a release which configures **vpdn ip udp ignore checksum** by default, if the user manually configures **no vpdn ip udp ignore checksum** in order NOT to ignore the checksum, this configuration change is not retained across reloads. After writing the configuration to NVRAM and reloading the router, the **vpdn ip udp ignore checksum** command will automatically be put back in place by IOS. This issue is seen on any image which contains the CSCef90365 fix and after configuring **no vpdn ip udp ignore checksum**.  
Workaround: Re-configure the **no vpdn ip udp ignore checksum** command after every reload.
- CSCsa52807: L2TP doing PMTUD vulnerable to spoofed ICMP paks.  
Symptoms: A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).  
These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml>

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>

## Resolved Caveats - Cisco IOS Release 12.3(8)YG1

- CSCef67682: Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

- 
- CSCeg25510: Image Agent: Router crashed during image upgrade  
Symptoms: A router crashes while downloading a file using the CNS Image Agent.  
This situation may be related to memory corruption or memory exhaustion.  
Conditions: This symptom is observed infrequently after the router has ran for a long time. One of the situations in which the symptom occurs is when you attempt to download an image file that does not exist on a TFTP server.  
Workaround: There is no workaround.
- CSCeg44078: C836 - DMZ - Delay transmitting traffic on the two ports Eth0 Eth2  
Symptoms: A Cisco 836 router may report a huge delay transmitting traffic on the two Ethernet interfaces (Ethernet 0 or 2).

Conditions: The problem is observed on a Cisco836 12.3(7)XR3 with DMZ.

Workaround: Administratively shut down both the ethernet0 and ethernet2 interfaces and then administratively bring up both these interfaces one after the other.

- CSCeg78458: Software forced crash due to CNS XML reload request

Symptoms: A Cisco 836 or Cisco 837 may reload because of a software-forced crash when you request a reload with an XML file via CNS.

Conditions: This symptom is observed with a CNS Configuration Engine version 1.4 that runs on an IE2115 server. The routers run Cisco IOS Release 12.3(8)YG. The symptom could also occur in Release 12.3.

Workaround: Enter the scheduler max-task-time 50000 command.

- CSCeg78674: Cisco IOS download causes meaningless con logs and malloc on CNS-EVENT bus

Symptoms: When you download a Cisco IOS image from CNS via an XML file to a Cisco 836 or Cisco 837, meaningless characters are generated on the router console and an invalid memory action with an associated traceback is generated on the CNS event bus.

Conditions: This symptom is observed with a CNS Configuration Engine version 1.4 that runs on an IE2115 server. The routers run Cisco IOS Release 12.3(8)YG. The symptom could also occur in Release 12.3.

Workaround: Enter the no logging cns-events command on the router. This command is enabled by default.

- CSCeg81454: CPU hog on reloading router

Symptoms: When you reload a Cisco 836 or a Cisco 837, a CPUHOG error may occur.

Conditions: This symptom is observed on a Cisco 836 and Cisco 837 that have a minimal configuration and no traffic load.

Workaround: Enter the scheduler max-task-time 50000 command.

- CSCeg87083: Root user (RBAC) fails to login as root while using a SSH connection

Symptoms: When entering via SSH, view-based users are not authorized to access their view but are authorized according to their corresponding privilege level.

Conditions: This symptom is observed on a Cisco platform that is configured for Role Based Access Control (RBAC).

Workaround: There is no workaround.

- CSCeg89937: Ethernet interface does not send ping replies after reload

Symptoms: Customer is sending continuous pings to ethernet0 interface from its laptop, which directly connected to fast ethernet port 1.

The issue here is that the pings get continuous timeouts...

[1] right after the reload of the c836

[2] not right after the reload, but the ping timeouts occur after >5min.

The fast ethernet port1 is not sending any traffic out anymore.

Condition: This issue has been seen with rommon 12.2(11r)YV1 and 12.2(11r)YV. The image used is c836-k9o3s8y6-mz.123-8.YG. Temporary fix of the issue for some minutes: Do a shut/no shut on the ethernet 2 interface. Ping are again working fine until again <5min. passes then you should see again timeouts.

Workaround: There is no workaround.

- CSCin80853: CNS prevents further configuration when interactive CLI applied

Symptoms: When an interactive configuration command is applied by the CNS Configuration Agent, the configuration is not applied correctly and the router cannot be configured any further. The reload command does not function either.

Conditions: These symptoms are observed when the CNS Configuration Agent is enabled with the `cns config` command and when the downloaded configuration includes an interactive configuration. Most configuration commands are NOT interactive. The following list of configuration commands are known to trigger the symptoms.

NOTE THERE MAY BE OTHER COMMANDS.

```
crypto ca authenticate (prompts the user for a "Yes/No" reply)
crypto key generate rsa (prompts the user for a numeric reply)
```

Workaround: Do not use an interactive configuration command via CNS. All interactive commands have a non-interactive equivalent, which you can discover by applying the desired configuration via the console of a router. Then, enter the `show running-config` command and look for the non-interactive form of the configuration command.

- CSCin82407: XAUTH failure and blank ACK can allow Phase 2 negotiation.

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

- CSCeg00277: Profile attributes are ignored when certificates are matched.

See note for CSCin82407 above.

- CSCef43691: L2TPv3 and UTI sessions doing PMTUD vulnerable to spoofed ICMP paks

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (`draft-gont-tcpm-icmp-attacks-03.txt`).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef60659: More stringent checks required for ICMP unreachable.  
See note for CSCef43691 above.
- CSCsa59600: IPSec PMTUD not working.  
See note for CSCef43691 above.
- CSCef44225: IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets.  
See note for CSCef43691 above.
- CSCef44699: GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets.  
See note for CSCef43691 above.
- CSCef61610: Incorrect handling of ICMPv6 messages can cause TCP performance problems.  
See note for CSCef43691 above.
- CSCsa61864: Enhancements to L2TPv3 PMTUD may not work.  
See note for CSCef43691 above.
- CSCef95695: No NAT-T UDP wrapper header packet is sent for different NAT-T version.  
Symptoms: ESP frames are sent as protocol 50 (ESP) instead of the UDP protocol that is required for NAT-T. (The Internet Key Exchange security association [IKE SA] is correctly established.) This symptom is observed when one peer runs Cisco IOS Release 12.3(8)YA or Release 12.3(11)T and uses NAT-T version 7, and another peer runs NAT-T version 2 or 3.  
Workaround: Remove NAT-T. Note that the symptom does not occur in Release 12.3(8)T4.
- CSCef68324: ICMPv6 pkt traceback  
Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.  
Cisco has made free software available to address this vulnerability for all affected customers.  
More details can be found in the security advisory posted at:  
<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

## Resolved Caveats - Cisco IOS Release 12.3(8)YG

- CSCeg32706: A traceback/memory leak occurs with IPSec performance testing.  
Symptoms: A Cisco router may exhibit a leak in process memory when running hardware encryption based IPSec. The leak only happens when you use IPSec with hardware encryption.  
Workaround: Use software encryption.
- CSCee73477: Spurious Access at show\_ip2access  
Symptoms: A traceback may be seen when the **show\_ip access-list** command is given, when named access lists are configured.  
Workaround: Use numbered access lists.

- CSCee83305: spurious access @dialer\_redial\_initiate found when config bri int  
Symptoms: A spurious access at dialer\_redial\_initiate is found when configured as BRI.  
Workaround: There is no workaround.
- CSCeg47738: Incorrect count loaded into Timer3 that handles ISDN layer1  
Symptoms: Incorrect count loaded into Timer3 that handles ISDN layer1.  
Workaround: There is no workaround.

## Additional References

The following sections describe the documentation available for the routers covered in these release notes. Documentation consists of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on [Cisco.com](http://www.cisco.com) and <http://www.cisco.com/univercd/home/index.htm>.

Use these release notes with these documents:

- [Release-Specific Documents](#)
- [Platform-Specific Documents](#)

## Release-Specific Documents

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

- [Cross-Platform Release Notes for Cisco IOS Release 12.3\(8\)T](#)

On [Cisco.com](http://www.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**



**Note** Cross-Platform Release Notes for Cisco IOS Release 12.3 T are located on [Cisco.com](http://www.cisco.com) 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 the following URL:  
<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 12.3T](#), which contain caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3T.

On [Cisco.com](http://www.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](http://www.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 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

Platform-specific documents are available on [Cisco.com](http://www.cisco.com) by following the appropriate Technical Documentation path below.

For Cisco SOHO 90 series and Cisco 830 series routers:

**Product Documentation: Routers: Fixed Config. Access Routers**

## 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

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feed-back, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

---

Use this document in conjunction with the documents listed in the “Additional References” 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.