



# Release Notes for Cisco 800 Series and Cisco SOHO 90 Series Routers for Cisco IOS Release 12.3(7)XR

---

**August 13, 2007**  
**Cisco IOS Release 12.3(7)XR7**  
**OL-8392-04**

These release notes describe new features and significant software components for the Cisco 800 series and Cisco SOHO 90 series routers that support the Cisco IOS Release 12.3(7)T, up to and including Release 12.3(7)XR7. 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](#) located on [Cisco.com](#).

For a list of the software caveats that apply to Release 12.3(7)XR7, see the “Caveats” section on page 12 and [Caveats for Cisco IOS Release 12.3\(7\)T](#). The online caveats document is updated for every maintenance release and is located on [Cisco.com](#).

## Contents

- [System Requirements, page 2](#)
- [New and Changed Information, page 7](#)
- [Caveats, page 12](#)
- [Related Documentation, page 35](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 40](#)



---

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

# System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(7)XR6 and includes the following:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 4](#)
- [Feature Set Tables, page 4](#)

## Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets that are supported by the Cisco IOS Release 12.3(7)XR6 on the Cisco 800 series and Cisco SOHO 90 series routers.

[Table 1](#) lists the memory requirements for Cisco IOS Release 12.3(7)XR6.

**Table 1** Recommended Memory for the Cisco 831, 836, 837, and Cisco SOHO 91, 96, and 97 Routers

Platform	Image Name	Feature Set	Image	Flash Memory		DRAM	
				Minimum	Recommended <sup>1</sup>	Minimum	Recommended
Cisco 831	Cisco 831 Series IOS IP/FW2 IPsec 3DES	IP/FW2/IPSec 3DES	c831-k9o3y6-mz	8 MB	12 MB	32 MB	48 MB
	Cisco 831 Series IOS IP/FW2 Plus IPsec 3DES	IP Plus/FW2/IPSec 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	8 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	8 MB	12 MB	32 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

**Table 1** Recommended Memory for the Cisco 831, 836, 837, and Cisco SOHO 91, 96, and 97 Routers (continued)

Platform	Image Name	Feature Set	Image	Flash Memory		DRAM	
				Minimum	Recommended <sup>1</sup>	Minimum	Recommended
Cisco SOHO 96	Cisco SOHO 96 Series IOS IP/FW/3DES	IP/FW 3DES	soho96-k9oy1-mz	8 MB	8 MB	32 MB	32 MB
Cisco SOHO 97	Cisco SOHO 97 Series IOS IP/FW 3DES	IP/FW 3DES	soho97-k9oy1-mz	8 MB	8 MB	32 MB	32 MB

1. Recommended memory is the memory required for potential future expansions.

## Hardware Supported

Cisco IOS Release 12.3(7)XR6 supports the following Cisco 800 series and Cisco SOHO 90 series routers:

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

For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 800 series and Cisco SOHO 90 series routers, which are available on [Cisco.com](http://www.cisco.com).

For the Cisco 800 series and Cisco SOHO 90 routers, click the following path:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_fix/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/index.htm)

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

For the Cisco 800 series routers and Cisco SOHO 90 series routers, click the following path:

**Technical Documentation: Routers: Fixed Config. Access Routers: <platform\_name>**

## Determining the Software Version

To determine which version of Cisco IOS software is currently running on your Cisco 800 series or Cisco SOHO 90 series router, log in to the router and enter the **show version** command. Using the Cisco 837 series router as an example, the following sample output from the **show version** command indicates the version number.

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C Software (C837-Y7-MZ), Version 12.3(7)XR6, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Synched to technology version 12.3(7.11)T
```

## Upgrading to a New Software Release

For general information about upgrading to a new software release, see [Cisco IOS Software Releases 12.3 T Installation and Upgrade Procedures](#) located on Cisco.com.

## Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.3(7)XR6 supports the same feature sets as Releases 12.3 and 12.3(7)T.



### Caution

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

Table 2 through Table 7 list the feature and feature sets supported in the Cisco IOS Release 12.3(7)XR6.

The tables use the following conventions:

- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, “12.3(7)XR” indicates that the feature was introduced in 12.3(7)XR. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.



### Note

These feature set tables contain only a list of selected features, which are cumulative for Release 12.3(7)nn early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image; additional features are listed in [Cross-Platform Release Notes for Cisco IOS Release 12.3\(7\)T](#) and in Release 12.3(7)T Cisco IOS documentation.

**Table 2** Feature Set for the Cisco 831 Router

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
Demilitarized Zone (DMZ) Port	12.3(7)XR1	Yes	Yes
<b>Easy VPN Remote Phase 4.0 Enhancements</b>			
Easy VPN with 802.1x Authentication	12.3(7)XR1	Yes	Yes
Easy VPN Remote with Certificates	12.3(7)XR1	Yes	Yes
Easy VPN Remote Backup Server List Autoconfiguration	12.3(7)XR1	Yes	Yes

**Table 2** Feature Set for the Cisco 831 Router (continued)

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
Easy VPN Remote Management Enhancements	12.3(7)XR1	Yes	Yes
Easy VPN Remote Load Balancing	12.3(7)XR1	Yes	Yes
Easy VPN Remote Multiple Subnet Support	12.3(7)XR1	Yes	Yes
Easy VPN Remote and Server on Same Interface	12.3(7)XR1	Yes	Yes
Easy VPN Remote and Site to Site on Same Interface	12.3(7)XR1	Yes	Yes
Easy VPN Perfect Forward Secrecy (PFS) via Policy Push	12.3(7)XR1	Yes	Yes
<b>Easy VPN Remote Phase 4.1 Enhancements</b>			
Easy VPN Dial Backup	12.3(7)XR2	Yes	Yes
Easy VPN Remote Traffic Triggered Activation	12.3(7)XR1	Yes	Yes

**Table 3** Feature Set for the Cisco 836 Router

Feature	In	Feature Set		
		IP/FW2 3DES	IP/FW2 Plus 3DES	IP Plus/FW2/Dial Backup IPSec 3DES
Demilitarized Zone (DMZ) Port	12.3(7)XR1	Yes	Yes	Yes
<b>Easy VPN Remote Phase 4.0 Enhancements</b>				
Easy VPN with 802.1x Authentication	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Remote with Certificates	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Remote Backup Server List Autoconfiguration	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Remote Management Enhancements	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Remote Load Balancing	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Remote Multiple Subnet Support	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Remote and Server on Same Interface	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Remote and Site to Site on Same Interface	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Perfect Forward Secrecy (PFS) via Policy Push	12.3(7)XR1	Yes	Yes	Yes
<b>Easy VPN Remote Phase 4.1 Enhancements</b>				
Easy VPN Dial Backup	12.3(7)XR1	Yes	Yes	Yes
Easy VPN Remote Traffic Triggered Activation	12.3(7)XR1	Yes	Yes	Yes

**Table 4** Feature Set for the Cisco 837 Router

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
Demilitarized Zone (DMZ) Port	12.3(7)XR1	Yes	Yes
<b>Easy VPN Remote Phase 4.0 Enhancements</b>			
Easy VPN with 802.1x Authentication	12.3(7)XR1	Yes	Yes
Easy VPN Remote with Certificates	12.3(7)XR1	Yes	Yes
Easy VPN Remote Backup Server List Autoconfiguration	12.3(7)XR1	Yes	Yes
Easy VPN Remote Management Enhancements	12.3(7)XR1	Yes	Yes
Easy VPN Remote Load Balancing	12.3(7)XR1	Yes	Yes
Easy VPN Remote Multiple Subnet Support	12.3(7)XR1	Yes	Yes
Easy VPN Remote and Server on Same Interface	12.3(7)XR1	Yes	Yes
Easy VPN Remote and Site to Site on Same Interface	12.3(7)XR1	Yes	Yes
Easy VPN Perfect Forward Secrecy (PFS) via Policy Push	12.3(7)XR1	Yes	Yes
<b>Easy VPN Remote Phase 4.1 Enhancements</b>			
Easy VPN Dial Backup	12.3(7)XR2	Yes	Yes
Easy VPN Remote Traffic Triggered Activation	12.3(7)XR1	Yes	Yes

**Table 5** Feature Set Table for the Cisco SOHO 91 Router

Feature	In	Feature Set	
		IP/FW 3DES	
PPP Random reconnect layer	12.3(7)XR	Yes	
X.25 over ISDN layer 2 reconnect function for SAPI 16	12.3(7)XR	No	
Inside to inside NAT	12.3(7)XR	Yes	
AZR enhancements	12.3(7)XR	No	

**Table 6** Feature Set Table for the Cisco SOHO 96 Router

Feature	In	Feature Set	
		IP/FW 3DES	
PPP Random reconnect timer	12.3(7)XR	Yes	
X.25 over ISDN layer 2 reconnect function for SAPI 16	12.3(7)XR	No	

**Table 6** Feature Set Table for the Cisco SOHO 96 Router (continued)

Feature	In	Feature Set
		IP/FW 3DES
Inside to inside NAT	12.3(7)XR	Yes
AZR enhancements	12.3(7)XR	No

**Table 7** Feature Set Table for the Cisco SOHO 97 Router

Feature	In	Feature Set
		IP/FW 3DES
PPP Random reconnect	12.3(7)XR	Yes
X.25 over ISDN layer 2 reconnect function for SAPI 16	12.3(7)XR	No
Inside to inside NAT	12.3(7)XR	Yes
AZR enhancements	12.3(7)XR	No

## New and Changed Information

The following sections list the new information about the Cisco 800 series and Cisco SOHO 90 series routers for Cisco IOS Release 12.3(7)XR. This information applies to Cisco IOS Releases 12.3(7)XR, 12.3(7)XR1, 12.3(7)XR2, 12.3(7)XR3, 12.3(7)XR4, 12.3(7)XR5, 12.3(7)XR6 and 12.3(7)XR7.

### New Software Features in Release 12.3(7)XR7

The Cisco IOS Release 12.3(7)XR7 supports the same software features that are supported in the Cisco IOS Release 12.3(7)XR6.

### New Software Features in Release 12.3(7)XR6

The Cisco IOS Release 12.3(7)XR6 supports the same software features that are supported in the Cisco IOS Release 12.3(7)XR5.

### New Software Features in Release 12.3(7)XR5

The Cisco IOS Release 12.3(7)XR5 supports the same software features that are supported in the Cisco IOS Release 12.3(7)XR4.

### New Software Features in Release 12.3(7)XR4

The Cisco IOS Release 12.3(7)XR4 supports the same software features that are supported in the Cisco IOS Release 12.3(7)XR3.

Note that Cisco 800 series routers were not supported under Cisco IOS Release 12.3(7)XR4.

## New Software Features in Release 12.3(7)XR3

The Cisco IOS Release 12.3(7)XR3 supports the same software features that are supported in the Cisco IOS Release 12.3(7)XR2.

## New Software Features in Release 12.3(7)XR2

The Cisco IOS Release 12.3(7)XR2 supports the same software features that are supported in the Cisco IOS Release 12.3(7)XR1.

## New Software Features in Release 12.3(7)XR1

The following sections describe the new software features supported by the Cisco 800 series routers for Release 12.3(7)XR1.

### Demilitarized Zone (DMZ) Port

The Demilitarized Zone (DMZ) Port feature permits two LAN networks instead of a single LAN network, which is currently available on the Cisco 830 series routers. This feature enables switch port 4 of the existing four 10/100 switch ports to be optionally used as a Layer 3 LAN port, thereby providing Cisco 830 series routers with one more 10-Mbps Layer 3 LAN port. The new LAN network port can be used for DMZ purposes for access to the customer's public Internet; web and other servers. The existing LAN network port will continue to be used for private internal traffic.

Typically, the DMZ port is configured at a lower security level than the LAN port connected to the Cisco 830 series router.

**Note**

---

The Ethernet 2 interface of the Cisco 830 series router should be used only as a DMZ port for LAN. Using the Ethernet 2 interface for WAN is not supported.

---

**Note**

---

The switch ports 1 through 4 are associated with the Ethernet 0 interface when the DMZ Port feature is not enabled. When the DMZ Port feature is enabled, only switch ports 1 through 3 are associated by means of the Ethernet 0 interface because switch port 4 is associated with the Ethernet 2 interface.

---

For more details, see the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xr7/dmz\\_port.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xr7/dmz_port.htm)

### Enabling DMZ Port

To enable the DMZ Port feature, turn on the Ethernet 2 interface. Enabling this feature converts the existing switch port 4 to a DMZ port, which is represented by the Ethernet 2 interface. Because switch port 4 provides DMZ functionality, it must be administratively up before this feature can be enabled. The

“Switch port 4 now connected to ethernet 2 interface” message is displayed on the router console when the DMZ Port feature is enabled. If the Ethernet 2 interface enabled and if you try to enable the Ethernet 2 interface again, no message will be displayed.

#### Example

```
Router(config)#interface fastethernet4
Router(config-if)#no shutdown
Router(config)#interface ethernet 2
Router(config-if)#no shutdown
Switch port 4 now connected to ethernet 2 interface.
```

### Disabling DMZ Port

The DMZ Port feature is turned off by disabling Ethernet 2 interface. Turning off this feature re-associates switch port 4 to the Ethernet 0 interface. The “Switch port 4 now connected back to ethernet 0 interface” message is displayed on the router console when the DMZ Port feature is disabled. If the Ethernet 2 interface disabled and if you try to disable the Ethernet 2 interface again, no message will be displayed.

#### Example

```
Router(config)#interface ethernet 2
Router(config-if)#shutdown
Switch port 4 now connected back to ethernet 0 interface
```

## Easy VPN Remote Phase 4.0 Enhancements

The following sections describe the Easy Virtual Private Network (VPN) Remote Phase 4.0 feature enhancements.

### Easy VPN with 802.1x Authentication

The Easy VPN with 802.1x Authentication feature enables *split tunneling*, which makes it possible for a corporate employee to connect to the corporate network while other persons using the same Internet connection will not have access to the protected tunnel to the corporate network.

For more information, see the following URL:

[http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/cli\\_t\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/cli_t_wp.htm)

### Easy VPN Remote with Certificates

Cisco IOS Release 12.3(7)XR and later releases support the Easy VPN Remote with Certificates feature, which uses public key infrastructure (PKI) and certificates to establish an IP Security (IPSec) connection.



#### Note

While configuring PKI on the remote router, use the same **subject-name** command for the subject name in the certificate; otherwise, the PKI will fail.

## Easy VPN Remote Backup Server List Autoconfiguration

The Easy VPN Remote feature allows configuration of multiple servers that the remote router will attempt to connect to. With this feature, the Easy VPN Server can “push” the server list to Easy VPN Remote clients, thus eliminating the need to manually configure the list of servers on all the Easy VPN Remote clients. Instead, only one server needs to be preconfigured on Easy VPN Remote client, and the rest of the server list will be pushed from the server to Easy VPN Remote client once the connection is established.

## Easy VPN Remote Management Enhancements

The Easy VPN Remote Management Enhancements feature simplifies the remote management of a Cisco IOS router that is acting as an Easy VPN Remote. This feature makes fully manageable the IP address that is pushed from the server at connect time. The pushed address is automatically assigned to a loopback interface that is dynamically created. This enables ping, Telnet, Simple Network Management Protocol (SNMP), and even dynamic routing to use the pushed IP address as the IP address for reaching the router. The user can design central site management solutions that use the pushed IP address as the IP address for reaching the remote routers. The Easy VPN Remote Management Enhancements feature can be enabled in both client and network extension modes.

## Easy VPN Remote Load Balancing

When configured with the Easy VPN Remote Load Balancing feature, an Easy VPN server will accept an incoming request from the Easy VPN Remote router at its virtual IP address. When the server is heavily loaded, it will send a “notify” message to the remote router which contains an IP address that represents a new peer that the client can connect to. The Easy VPN Remote router receives this “redirect” message and will attempt to connect to a different server at the address contained in the notify message.

## Easy VPN Remote VLAN Support

The Easy VPN Remote Virtual LAN (VLAN) Support feature allows you to define a VLAN as an Easy VPN Remote inside, or private interface. This VLAN may be an internal VLAN on the remote router. That is, when defined, IP Security (IPSec) security association (SA) will be established for the VLAN inside interface.

## Easy VPN Remote Multiple Subnet Support

The Easy VPN Remote Multiple Subnet Support feature allows multiple subnets to be defined to Easy VPN on a single inside interface on the Easy VPN remote router. The subnets can be multiple hops away from the inside LAN interface. The subnets must be manually configured because they cannot be learned by dynamic routing. The Easy VPN Remote Multiple Subnet Support feature is supported in client mode only.

## Easy VPN Remote and Server on Same Interface

The Easy VPN Remote and Server on Same Interface features allows you to configure Easy VPN Remote functions and Easy VPN Server functions on the same interface. A typical application is a remote router that acts as a client to the Easy VPN server at headquarters, while also acting as a server for local software clients. Such a router has a single public interface to the Internet; both the server and client functions are configured on the same interface.

## Easy VPN Remote and Site to Site on Same Interface

The Easy VPN Remote and Site to Site on Same Interface feature allows you to configure Easy VPN Remote functions and site-to-site (standard IPSec) functions on the same interface. A typical application is a remote router that acts as a client to the Easy VPN server at headquarters, while also having a site-to-site tunnel.

## Easy VPN Perfect Forward Secrecy (PFS) via Policy Push

The Easy VPN Perfect Forward Secrecy (PFS) via Policy Push feature allows PFS for the Easy VPN connection to be configured dynamically the connect time by means of MODCFG policy push from the server.

## Easy VPN Remote Phase 4.1 Enhancements

The following sections describe the Easy Virtual Private Network (VPN) Remote Phase 4.1 feature enhancements.

### Easy VPN Dial Backup

The Easy VPN Dial Backup feature enables Cisco IOS software to identify when the primary Internet connection goes down and initiate a dial-on-demand routing (DDR) connection to a preconfigured destination from any alternative WAN/LAN port. The Easy VPN Dial Backup feature is typically used for deployments in which a remote router has a single dedicated VPN connection over the Internet, but can dial up to an ISP if the primary link goes down.

The Easy VPN Dial Backup feature allows an object to be tracked (by IP address or host name) by means of periodic pings and allows installation or removal of the static route, based on the state of the tracked object. If the Internet connectivity is lost—that is, if the pings fail—the default route for the primary interface is removed and the floating static route for the backup interface becomes the preferred route. This triggers the dialer interface to come up and connect to the ISP. While in backup mode, the pings are still sent to the primary interface. When the ping is successful, again the primary connection will be restored and back up tunnel will be disconnected. The dial-up connection will time out, based on the idle timer settings of the dialer interface.

An advantage of the Easy VPN Dial Backup feature is it works without requiring that a dynamic routing protocol to be running across the VPN to test connectivity.

### Easy VPN Remote Traffic Triggered Activation

The Easy VPN Remote Traffic Triggered Activation feature introduces a new method of activating Easy VPN tunnels, based on the user traffic. This feature brings up the tunnel only when there is traffic. This feature can also be used with an idle timer on the tunnel to bring the tunnel up or down when required.

## New Software Features in Release 12.3(7)XR

There are no new software features supporting the Cisco 800 series and Cisco SOHO 90 series router for Release 12.3(7)XR.

## New Software Features in Release 12.3(7)T

For information regarding the features supported in Cisco IOS Release 12.3(7)T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on [Cisco.com](http://www.cisco.com):

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

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

**Service & Support: Technical Documents: Cisco IOS Software: Release 12.3: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.3(7)T)**

## 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 in Cisco IOS Release 12.3(7)T are also in Release 12.3(7)XR7. For information on caveats in Cisco IOS Release 12.3(2)T, see the *Caveats for Cisco IOS Release 12.3(7)T* document. This document lists severity 1 and 2 caveats; the documents is located on [Cisco.com](http://www.cisco.com).



### 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 - Release 12.3(7)XR7

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>

CSCsj44081 Improvements in diagnostics and instrumentation

**Symptom** Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS Software releases published after April 5, 2007.

**Details** With the new enhancement in place, IOS will emit a [%DATACORRUPTION-1-DATAINCONSISTENCY](#) error message whenever it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

The [%DATACORRUPTION-1-DATAINCONSISTENCY](#) error message is preceded by a timestamp

May 17 10:01:27.815 UTC: [%DATACORRUPTION-1-DATAINCONSISTENCY](#): copy error

The error message is then followed by a traceback.

It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

**Recommended Action** Collect "show tech-support" command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the [%DATACORRUPTION-1-DATAINCONSISTENCY](#) message and note those to your support contact.

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

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

**Symptom 1:** 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.

**Condition 1:** 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.

**Workaround 1:** 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.

**Symptom 2:** 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.

**Condition 2:** 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.

**Workaround 2:** 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.

CSCsi67763 IPS evasion using Unicode encoding for HTTP-based attacks

**Symptom** The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

<http://www.kb.cert.org/vuls/id/739224>

By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

Cisco response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml>

CSCsg16908 IOS FTP Server Deprecation

**Symptom** 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 aaron Buffer overflow in NHRP protocol

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>.

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>.

CSCsb93407 H323 port tcp 1720 still listening after call service stop

**Symptom** 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.

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).

CSCsh58082 SIP: A router may reload due to SIP traffic

**Symptom** 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>.

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>

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>

CSCef77013 tighter parameter checking for ipv6 CSCsi01470 iwijnand Crafted MDT Data Join TLV in VRF causes multicast state in core

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>

CSCeh73049 tclsh mode bypasses aaa command authorization check

**Symptom** 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>

CSCek26492 ansjory Enhancements to Packet Input Path.

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

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

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

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

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

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/en/US/products/products\\_security\\_advisory09186a00809bb300.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a00809bb300.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>

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>.

CSCsd81407 Router crash on receiving abnormal MGCP messages CSCse85200 padchand  
Inadequate validation of TLVs in cdp

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>.

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 thru 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.

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

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

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

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                        000000000111111111112222222222333^
                        12345678901234567890123456789012|
                                                                |
                                                                PROBLEM
                                                                (Variable Overflowed).
```

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

CSCsh46705 Remove unused func declaration of  
vtsp\_tsp\_call\_disconnect\_ind\_rawsignal

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.

CSCsj52927 DATACORRUPTION-1-DATAINCONSISTENCY message in show log CSCsj66550  
rclousto Strcpy off by one in appn/eis\_command.c:1075

**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.

CSCsj66513 Traceback detected at DNQueuePeers CSCsj72800 dwind Unbounded strcpy  
in alps/alps\_chain.c:636 (conn\_isp) CSCsh22430 richc c82x and c83x MMU mapping  
refinement

**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** No workaround

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.

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](#)

**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>

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.

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>

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/en/US/products/products\\_security\\_advisory09186a00809bb300.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a00809bb300.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 messag

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/en/US/products/products\\_security\\_advisory09186a00809bb300.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a00809bb300.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>.

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

**Symptom** 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.

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#wp1027129](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cntrl_acc_vtl.html#wp1027129)

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>

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.

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.

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>

CSCei62522 ISAKMP SA negotiation not successful in aggressive mode with RADIUS

**Symptom** ISAKMP SA negotiation is not successful in aggressive mode.

**Conditions** This symptom has been observed when testing Radius Tunnel Attribute with HUB and Spoke Scenario using Cisco IOS interim Release 12.4(3.3).

**Workaround** There is no workaround.

CSCed94829 IOS reloads due to malformed IKE messages

Multiple Cisco products contain vulnerabilities in the processing of IPsec IKE (Internet Key Exchange) messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) "PROTOS" Test Suite for IPsec and can be repeatedly exploited to produce a denial of service.

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

This advisory is posted at <http://www.cisco.com/warp/customer/707/cisco-sa-20051114-ipsec.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/en/US/products/products\\_security\\_advisory09186a00809bb300.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a00809bb300.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>.

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>

CSCej20505 Router hangs with overly large 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>.

CSCeg62070 Tracebacks noticed with Radius configs through HTTP Post

**Symptom** Tracebacks or crash are seen during HTTP transactions with long URLs.

**Conditions** The crash is seen when the length of any token in the URL of the request is excessively long.

**Conditions** Disable HTTP server using the **no ip http server** command.

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.

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>.

CSCsd34855 VTP update with a VLAN name >100 characters causes buffer overflow

**Symptom** The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

**Conditions** The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

**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 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>

CSCsd40334 IPv6 packet can cause crash

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. 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>

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>.

CSCsk73104

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

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

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>.

## Resolved Caveats - Release 12.3(7)XR6

- CSCei61732

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>.

- CSCeg15044

Not able to telnet to card (No Free TTYs error).

- CSCsa54608

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.

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

This advisory will be 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)

## Resolved Caveats - Release 12.3(7)XR5

- 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>

- CSCee45312

Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method of none can be bypassed.

Systems that are configured for other authentication methods or that are not configured with a fallback method of none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and a fallback method of none are vulnerable to this issue. Some configurations using RADIUS, fallback method none, and an additional method are not affected.

Cisco has made free software available to address this vulnerability.

More details can be found in the security advisory which posted at the following URL <http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml>

- CSCeh13489

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 the event is recorded in the log.

- CSCin74088

Problem: memory not being freed correctly for ezvpn\_process.

Symptom: "sh processes memory <pid of ezvpn client process>" will display the memory not being freed for the ezvpn client process. Ezvpn works fine.

- CSCsa40962

A Cisco IOS router acting as an EzVPN server that terminates vpn client sessions may experience a memory leak in the processor memory pool. This can be identified by an increasing amount of memory held by the Crypto IKMP process in the **show process memory** output.

## Resolved Caveats - Release 12.3(7)XR4

- CSCeg44078

A Cisco836 router may report a huge delay transmitting traffic on the two Ethernet interfaces (Ethernet 0 or 2). The problem has been observed with 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.

- CSCeg89937  
Ethernet interface does not send ping replies after reload.
- CSCeh89139  
IPSEC real time DNS : unable to resolve peer hostname.  
With the IPSEC realtime DNS feature, when resolving the hostname, the router tries to do a ISAKMP SA negotiation and both fail (negotiation and name resolving).
- CSCed03333  
CBAC FTP-data sessions remain in SIS\_CLOSING state.  
Workaround: Lowering the inspect FTP timeout and disabling CEF will reduce exposure. Bump certain out-of-order packets to process path for catch-up and then drop packets if unsuccessful.
- CSCee47441  
CBAC inspection causes software-forced reload.  
When the Cisco IOS Firewall CBAC is configured, the router may have a software-forced reload caused by one of the inspections processed. This symptom is observed when the router is part of a DMVPN hub-spoke with a Cisco VoIP phone solution deployed on it, and the router is connected to the central office over the Internet. The Cisco VoIP phone runs the SKINNY protocol.  
Workaround: None.
- CSCee67450  
BGP error msg trackback.  
A device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a DoS attack from a malformed BGP packet. Only devices with the command **bgp log-neighbor-changes** configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.  
Cisco has made free software available to address this problem. Please see the advisory available at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>.
- CSCef81501  
Crash occurs while scaling L2TPv3 Xconnect commands on subinterfaces.  
When L2TPv3 tunnels are scaled and the IP Path MTU Discovery feature is enabled, a memory leak and crash may occur. This symptom is observed when multiple Xconnect statements are applied in conjunction with the IP Path MTU Discovery feature in the pseudowire class.  
Workaround: Do not enable the IP Path MTU Discovery feature in an L2TPv3 configuration.
- CSCeg01740  
Crash when L2TPv3 manual session delete.  
A router crashes when you delete a manual static Xconnect service with L2TPv3 encapsulation.  
Workaround: Do not delete a manual static Xconnect service with L2TPv3 encapsulation.
- 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>.

- CSCef44225  
IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets.  
See note for CSCef43691 above.
- CSCef60659  
More stringent checks required for ICMP unreachable.  
See note for CSCef43691, above.
- CSCsa59600  
IPSec PMTUD not working [after CSCef44225].  
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.
- CSCsa52807  
L2TP doing PMTUD vulnerable to spoofed ICMP paks.  
See note for CSCef43691, above.
- CSCsa61864

Enhancements to L2TPv3 PMTUD may not work [Follow-up to CSCef43691]  
See note for CSCef43691, above.

## Resolved Caveats - Release 12.3(7)XR3

- CSCed78149

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>.

- CSCef46191

Unable to telnet.

A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

The Advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

- CSCed78217

Add Survivable Remote Site Telephony (SRST) call pickup based on called number match.

- CSCee05720

Interactive CLI: **show run** command not returning the full configuration.

Commands initiated via the **cons exec** command-line interface (CLI) command do not run at the correct privilege level. This results on some commands not being permitted.

**Workaround:** None.

- CSCec88490

Cosmetic Display CLI Related Issues.

While giving **line-mode 2-wire ?** command in ATM mode on WIC-1SHDSL-V2, the help text displays incorrect mapping between the line number and the pins used.

**Workaround:** None.

- CSCee03847

WRED-COUNT: Wrong instance value created for [**rate-limit**] command.

Weighted random early detection (WRED) counter fails.

**Workaround:** None.

- CSCee34422

Shutting down the backup CCM causes major calls drop.

When the second backup Cisco CallManager (CCM) is down during active load testing, none of the active calls can be sustained.

**Workaround:** None.

- CSCee65576

Bus error in crypto ip\_vrf\_pak\_subblock\_copy.

A router running IP Security (IPSec) may reload due to a bus error.

**Workaround:** Enter **no ip-virtual reassembly** command on the router.

- CSCef06389

8172A590 chunkmagic 0 chunk\_freemagic 1000000 tracebacks.

A Cisco router that is configured as a spoke in a hub-spoke network shows tracebacks.

**Workaround:** None.

- CSCef28703

Router crashes when show controller ethernet CLI is executed.

A Cisco 1700 series router crashes when **show controller ethernet** command is entered.

**Workaround:** None.

- CSCef49904

SNMP-server trap source loopback0 traps sourced from the wrong interface.

- CSCin74147

Sometimes EZVPN does not accept XAuth request from server.

Easy Virtual Private Network (EZVPN) may not prompt for extended authentication (XAuth) credentials on console.

**Workaround:** Enter the **clear crypto ipsec client ezvpn** command and reconnect if it is in manual mode.

- CSCin82407

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 will be posted to

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

## Caveats - Release 12.3(7)XR2

There are no caveats specific to Cisco IOS Release 12.3(7)XR2 that require documentation in the release notes.

## Caveats - Release 12.3(7)XR1

There are no caveats specific to Cisco IOS Release 12.3(7)XR1 that require documentation in the release notes.

## Caveats - Release 12.3(7)XR

There are no caveats specific to Cisco IOS Release 12.3(7)XR that require documentation in the release notes.

## Related Documentation

The following sections describe the documentation available for the Cisco 800 series and Cisco SOHO 90 series routers. These documents consist 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](#)
- [Cisco Feature Navigator](#)

## 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\(7\)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 this 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

These documents are available for the Cisco 800 series routers:

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

**Technical Documentation: Routers: Fixed Config. Access Routers: <platform\_name>**

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

**Product Documentation: Routers: Fixed Config. Access Routers: <platform\_name>**

These documents are available for the Cisco 1700 series routers:

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

**Products and Solutions: Routers: Cisco 1700 Series Modular Access Routers**

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

**Product Documentation: Routers: Modular Access Routers: Cisco 1700 Series Routers**

## Cisco Feature Navigator

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

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

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

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

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

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

### Documentation Modules

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

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

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

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

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

### Cisco IOS Release 12.3 Documentation Set Contents

[Table 8](#) lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.

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

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

On <http://www.cisco.com/univercd/home/index.htm> at:  
**Cisco IOS Software: Cisco IOS Release 12.3**

**Table 8 Cisco IOS Release 12.3 Documentation Set**

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

**Table 8 Cisco IOS Release 12.3 Documentation Set (continued)**

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

**Table 8 Cisco IOS Release 12.3 Documentation Set (continued)**

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

## Obtaining Documentation, 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 “Related Documentation” section.

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

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

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

© 2007, Cisco Systems, Inc. All rights reserved