



Release Notes for Cisco 1700 Series Routers for Cisco IOS Release 12.3(8)XX2e

August 08, 2007

0L-6269-09

These release notes cover the limited release of the c1700-advsecurityk9-mz image for Cisco 1700 series routers.

New features and significant software components for the Cisco 1700 series routers that support the Cisco IOS Release 12.3(8)T, up to and including Cisco IOS Release 12.3(8)XX2E, are documented. 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 Cisco IOS Release 12.3(8)XX2E, see the “[Caveats](#)” [section on page 7](#) and [Caveats for Cisco IOS Release 12.3\(8\)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 5](#)
- [Limitations and Restrictions, page 7](#)
- [Caveats, page 7](#)
- [Additional References, page 37](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 39](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(8)XX2E and includes the following sections:

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

Memory Requirements

[Table 1](#) describes the memory requirements for the Cisco IOS feature sets that are supported by the Cisco IOS Release 12.3(8)XX2E on the Cisco 1700 series routers.

Table 1 *Recommended Memory for the Cisco 1700 Series Routers—Cross-Platform Images*

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 1721, 1751, 1751-V, 1760, 1701, 1711, 1712	Cisco 1700 IOS Advanced Security	Advanced Security	c1700-advsecurityk9-mz	16 MB	64 MB

Hardware Supported

Cisco IOS Release 12.3(8)XX2E supports the following Cisco 1700 series routers:

- Cisco 1701 router
- Cisco 1711 router
- Cisco 1712 router
- Cisco 1721 router
- Cisco 1751 and 1751-V routers
- Cisco 1760 router

The Cisco 1701, Cisco 1711, Cisco 1712, and Cisco 1721 routers run only data images. The Cisco 1751, Cisco 1751-V, and Cisco 1760 routers run data or data-and-voice images, providing digital and analog voice support. The Cisco 1711 and Cisco 1712 routers run select IP Security (IPSec) Triple Data Encryption Standard (3DES) images only (the Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES, the Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 3DES, the Cisco 1700 IOS ADVANCED SECURITY, the Cisco 1700 IOS ADVANCED IP SERVICES, and the Cisco 1700 IOS ADVANCED ENTERPRISE SERVICES images).

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 1700 series routers. These documents are available on Cisco.com at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

Determining the Software Version

To determine which version of the Cisco IOS software is currently running on your Cisco 1700 series router, log in to the router and enter the **show version** command. The following sample output from the show version command indicates the version number.

```
Router> show version
Cisco Internetwork Operating System Software
Cisco IOS Software, C1700 Software (C1700-Y7-MZ), Version 12.3(8)XX2e, 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(8)XX2D supports the same feature sets as Releases 12.3 and 12.3(8)T, but Release 12.3(8)XX2D includes new features supported by the Cisco 1700 series routers. Cisco IOS Release 12.3(8)XX2E is a rebuild of Release 12.3(8)XX2D and includes only bug fixes; it does not include any new features.

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.

Table 2 through Table 4, Part 2 list the feature and feature sets supported in the Cisco IOS Cisco IOS Release 12.3(8)XX2E. 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(8)XX2D” indicates that the feature was introduced in Release 12.3(8)XX2D. 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 a list of selected features that are cumulative for Release 12.3(8)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\(8\)T](#) and in Release 12.3(8)T Cisco IOS documentation.

Table 2 Feature List by Cisco 1700 Legacy Feature Set for Cisco 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set		
		IP/ADSL/VOX PLUS	IP/ADSL/VOX/FW/IDS PLUS IPSEC 3DES	IP/ADSL/IPX/AT/IBM/VOX/FW/IDS PLUS IPSEC 3DES
ARP ¹ —Auto Logoff	12.3(8)XX2D	Yes	Yes	Yes

1. ARP = Address Resolution Protocol.

Table 3 Feature List by Cisco 1700 Legacy Feature Set for Cisco 1721, 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set					
		IP	IP/ADSL	IP/ADSL PLUS	IP/ADSL/IPX/AT/IBM PLUS	IP/ADSL/FW/IDS PLUS IPSEC 3DES	IP/ADSL/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES
ARP—Auto Logoff ¹	12.3(8)XX2D	Yes	Yes	Yes	Yes	Yes	Yes

1. The ARP—Auto Logoff feature is not supported on Cisco 1720 router.

Table 4, Part 1 Feature List by Cross-Platform Feature Set for Cisco 1701, 1711, 1712, 1721, 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set				
		ADVANCED IP SERVICES	SP SERVICES	ENTERPRISE SERVICES	ADVANCED ENTERPRISE SERVICES	IP BASE
ARP—Auto Logoff	12.3(8)XX2D	Yes	Yes	Yes	Yes	Yes

Table 4, Part 2 Feature List by Cross-Platform Feature Set for Cisco 1701, 1711, 1712, 1721, 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set		
		ENTERPRISE BASE	ADVANCED SECURITY	IP VOICE ¹
ARP—Auto Logoff	12.3(8)XX2D	Yes	Yes	Yes

1. This image is supported only on Cisco 1751, 1751-V, and 1760 routers.

New and Changed Information

Cisco IOS Release 12.3(8)XX2C supports the features described in this section.

New Hardware Features in Cisco IOS Release 12.3(8)XX2E

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.3(8)XX2D

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.3(8)XX2D

There are no new software features in this release.

New Software Features in Cisco IOS Release 12.3(8)XX2C

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.3(8)XX2b

There are no new software features in this release.

New Software Features in Cisco IOS Release 12.3(8)XX2a

There are no new software features in this release.

New Software Features in Cisco IOS Release 12.3(8)XX2

There are no new software features in this release.

New Software Features in Cisco IOS Release 12.3(8)XX1

There are no new software features in this release.

New Software Features in Cisco IOS Release 12.3(8)XX

The following sections describe the new software features supported by the Cisco 1700 series routers for Cisco IOS Release 12.3(8)XX.

ARP—Auto Logoff

The Address Resolution Protocol (ARP)—Auto Logoff feature overcomes a limitation of the current Authorized ARP Feature which causes premature log-off of peers. The ARP—Auto Logoff feature provides control for the probing of authorized peers, thus yielding more accurate detection of a peer's state of activity. The ARP—Auto Logoff feature permits configuration of how soon (*interval*) a peer will be probed and the maximum number of probes (*count*).

The new ARP probe function is enabled on an interface by the new interface configuration command **arp probe interval** <1-10> **count** <1-60>. The **no** form of the command is used to disable the function. The configuration is limited to, but not enforced on, the interface that has authorized ARP running.

The *interval* value specifies how soon a peer router will be probed if no reply is received from it. The *count* specifies the maximum number of probes.

The probing of a peer is triggered by the ARP timeout value for the interface. This value is calculated by the ARP timestamp and the configured ARP timeout value on the interface. Therefore, the actual probe starting time is calculated on the basis of the last ARP reply probe received from the peer.

To verify that the ARP probing process is running, use the **show cpu process | in ARP** command.

New Software Features in Cisco IOS Release 12.3(8)T

For information regarding the features supported in Cisco IOS Release 12.3(8)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/ios123/123relnt/xprn123/index.htm>

Limitations and Restrictions

The following sections describe the limitations and restrictions that apply to the Cisco 1700 series routers for Cisco IOS Cisco IOS Release 12.3(8)XX2E.

ARP—Auto Logoff

The ARP—Auto Logoff feature requires authorized ARP, DHCP, and secure ARP to be enabled on the interface.

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(8)T are also in Cisco IOS Cisco IOS Release 12.3(8)XX2E. For information on caveats in Cisco IOS Release 12.3(2)T, see the [Caveats for Cisco IOS Release 12.3\(8\)T](#) document. This document lists severity 1 and 2 caveats; the documents is located on [Cisco.com](#).

**Note**

If you have an account with [Cisco.com](#), you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](#) and go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Resolved Caveats - Cisco IOS Release 12.3(8)XX2e

CSCsd81407

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>

CSCsg70474

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>

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>.

CSCsi60004

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

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>

CSCef77013

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 Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco 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>.

CSCsj66513 Traceback detected at DNQueuePeers

Symptom Traceback found at DNQueuePeers

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

Workaround There is no workaround

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

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

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

For example:

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

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

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

CSCsj52927 DATACORRUPTION-1-DATAINCONSISTENCY message in show log

Symptom DATACORRUPTION-1-DATAINCONSISTENCY messages are seen in 'show log'.

Conditions The messages are seen when the router comes up.

Workaround There is no workaround.

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.

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.

CSCsj16292 DATACORRUPTION-1-DATAINCONSISTENCY: copy error

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

`%DATACORRUPTION-1-DATAINCONSISTENCY: copy error-Traceback=`

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

Workaround There is no workaround.

CSCef61610 Incorrect handling of ICMPv6 messages can cause TCP performance problems

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>.

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>

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>

CSCef48336 Corrupted OSPF Hello packets caused software forced crash

OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89. A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

Using OSPF Authentication can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice. A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack.

Workaround Using OSPF Authentication OSPF authentication may be used as a workaround. OSPF packets without a valid key will not be processed. MD5 authentication is highly recommended, due to inherent weaknesses in plain text authentication. With plain text authentication, the authentication key will be sent unencrypted over the network, which can allow an attacker on a local network segment to capture the key by sniffing packets.

Refer to <http://www.cisco.com/warp/public/104/25.shtml> for more information about OSPF authentication. Infrastructure Access Control Lists Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a

network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection ACLs: <http://www.cisco.com/warp/public/707/iacl.html>

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

For further information about deploying access lists, see the “Protecting Your Core: Infrastructure Protection Access Control Lists” document at: <http://www.cisco.com/warp/public/707/iacl.html>.

For information about using control plane policing to block access to TCP port 1720, see the “Deploying Control Plane Policing White Paper” at: http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml.

CSCsf28840 Crash due to configured peer type control vector

A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

There are workarounds available for this vulnerability.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml>

CSCsa54608 IOS Firewall Auth-Proxy for FTP/Telnet Sessions buffer overflow

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition. Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected. Only devices running certain versions of Cisco IOS are affected. 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

CSCee45312 Radius authentication bypass when configured with a none fallback method

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 to none can be bypassed. Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

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

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

CSCei61732 Additional data integrity check in system timer

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>

CSCef68324 ICMPv6 pkt traceback

Cisco Internetwork Operating System (IOS®) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation. Cisco has made free software available to address this vulnerability for all affected customers. More details can be found in the security advisory that is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>

CSCsj18014 Caller ID string received with extra characters

Symptom A caller ID may be received with extra characters.

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

Workaround There is no workaround.

CSCsb79076 MGCP RSVP enabled calls fails due to spurious error @ qosmodule_main
 %SYS-3-TIMERNEG errors and tracebacks are observed while making MGCP RSVP calls on a analog (RGW) setups. Observed in 12.4(3.9)T1 IOS version.

Workaround There is no workaround.

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.

CSCin95836 Buffer overflow in NHRP protocol

Symptom A Cisco IOS device configured for NHRP may restart.

Workaround There is no workaround.

Resolved Caveats - Cisco IOS Release 12.3(8)XX2d

CSCs#04754

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>

CSCin95836

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>.

CSCsb12598

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>.

CSCsb40304

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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



Note

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

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

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

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

CSCsd85587

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)

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

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

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



Note

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

CSCsd92405

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

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

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

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

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

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



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

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

CSCed95187 IP ID field is predictable for connectionless RST packets

Symptom RST packets sent in response to a TCP SYN packet received by the device on a non-listening port contain a non-randomized Identification value on the IP header.

Conditions There are no special conditions

Workaround There is no workaround.

Further Problem Description: From RFC791, the description of the Identification field is:

Identification

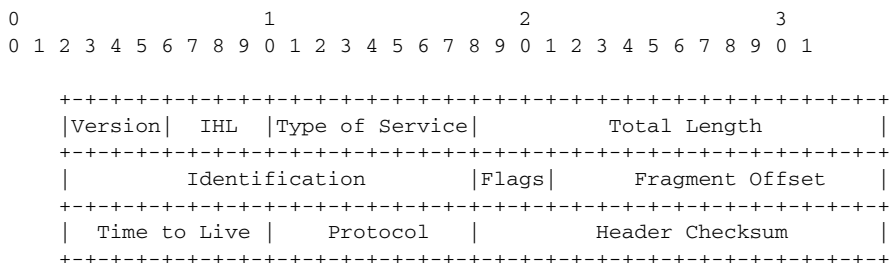
The choice of the Identifier for a datagram is based on the need to provide a way to uniquely identify the fragments of a particular datagram. The protocol module assembling fragments judges fragments to belong to the same datagram if they have the same source, destination, protocol, and Identifier. Thus, the sender must choose the Identifier to be unique for this source, destination pair and protocol for the time the datagram (or any fragment of it) could be alive in the internet. It seems then that a sending protocol module needs to keep a table of Identifiers, one entry for each destination it has communicated with in the last maximum packet lifetime for the internet.

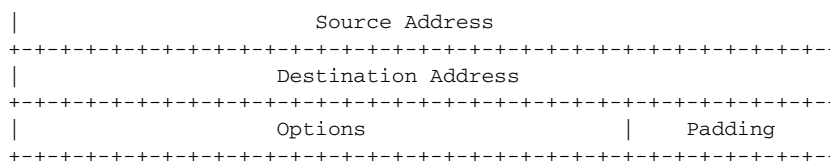
Also from RFC791: The IP ID is before the flags and fragment offset fields.

For Example: Internet Datagram header

3.1. Internet Header Format

A summary of the contents of the internet header follows:





CSCse95758 Access Lists support for all CONFIG-COPY-MIB protocols under snmp-server

Symptom Customers can use an access list to restrict TFTP configuration transfers that are initiated via SNMP by using the command `snmp-server tftp-server-list access-list`. This restriction is not possible for the FTP, RCP, and SCP protocols.

Conditions This symptom is observed on any Cisco IOS platform that is configured for SNMP. The following sample configuration causes the platform to reject configuration file transfers via SNMP from all hosts except the TFTP server that is specified in access list 5: `snmp-server tftp-server-list 5`:

```

access-list 5 permit 10.1.1.1
snmp-server community private RW 5
snmp-server tftp-server-list 5

```

Workaround Follow these workarounds:

1. Apply a more general access list to restrict traffic to and from the affected platform.
2. Disallow configuration copy from SNMP by excluding CISCO-CONFIG-COPY-MIB using `snmp views`.
3. Disable the SNMP server.

Fixed Software Information:

Access-List Support for CISCO-CONFIG-COPY-MIB The `snmp-server file-transfer access-group` command is introduced to restrict configuration transfers that are initiated via the Simple Network Management Protocol (SNMP). Supported transfer protocols are TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP).

This command replaces the `snmp-server tftp-server-list` command.

For detailed information about the `snmp-server file-transfer access-group` command, see the Cisco IOS Network Management Command Reference, Release 12.4.

CSCek26492 Enhancements to Packet Input Path.

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

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

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

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

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

CSCsd92405 Router crashed by repeated SSL connection with malformed finished message

Symptom A router crashes when receiving multiple malformed TLS and/or SSL3 finished messages. A valid username and password are not required for the crash to occur.

Conditions This symptom is observed when a router has HTTP secure server enabled and has an open, unprotected HTTP port.

Workaround There is no workaround. Minimize the chances of the symptom occurring by permitting only legitimate hosts to access HTTP on the router.

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>.

CSCed09685 IOS should not send passwords and sensitive information to ACS logs.

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

Conditions This problem happens only with command accounting enabled.

Workaround Disable command accounting.

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.

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>

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



Note 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.

Conditions 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.

Conditions 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.

CSCsg70355 Adopt new default summer-time rules from Energy Policy Act of 2005

Symptom Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.

Conditions The Cisco IOS configuration command:

clock summer-time zone

recurring

uses United States standards for daylight savings time rules by default. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March. It changes the end date from the last Sunday of October to the first Sunday of November.

Workaround A workaround is possible by using the clock summer-time configuration command to manually configure the proper start date and end date for daylight savings time. After the summer-time period for calendar year 2006 is over, one can for example configure:

clock summer-time PDT

recurring 2 Sun Mar 2:00 1 Sun Nov

2:00

(This example is for the US/Pacific time zone.)

Not A Workaround: Using NTP is not a workaround to this problem. NTP does not carry any information about timezones or summertime.

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/products/ps6441/products_configuration_guide_chapter09186a0080716c2.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

<http://www.cisco.com/warp/public/707/ssh.shtml>

CSCse85200 Inadequate validation of TLVs in cdp

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

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

Workaround Workaround is to disable on interfaces where CDP is not necessary.

CSCsa43465 None method in default login method list allows enabling with no passwd

Symptom Users may be able to access root view mode (privilege level) 15 without entering a password.

Conditions This symptom is observed on a Cisco router that has the Role-Based CLI Access feature enabled and occurs when the none keyword is enabled in the default login method list.

For example, the symptom may occur when you enter the **aaa authentication login default group tacacs+ none**. When the TACACS+ server is down, users are allowed to enter non-privileged mode. However, users can also access the root view through the **enable view** command without having to enter a password.

Workaround Ensure that the **none** keyword is not part of the default login method list.

Further Problem Description: The fix for this caveat places the authentication of the **enable view** command in the default login method list.

CSCse04560 tftp-server allows for information disclosure

Symptom A tftp client trying to transfer a file from a Cisco IOS device configured as a tftp server and which is denied by an ACL receives a different result depending if the file is being offered for download or not. This may allow a third party to enumerate which files are available for download.

Conditions The **tftp-server** command is configured on the device and an ACL restricting access to the file in question has been applied as in this example:

```
tftp-server
flash:filename1
access-list-number
access-list access-list-
number
permit 192.168.1.0
0.0.0.255
access-list access-list-
number
deny any
```

Workaround The following workarounds can be applied:

1. Interface ACLConfigure and attach an access list to every router interface active and configured for IP packet processing. For Example:

```
access-list access-list-
number
remark --- the following hosts
and networks area
ALLOWED for TFTP access
access-list access-list-
number
permit udp host
source_1
host
interface_address_1
eq 69
access-list access-list-
number
permit udp host
source_2
host
interface_address_2
eq 69
access-list access-list-
number
permit udp source source-
wildcard
```

```

host
interface_address_1
eq 69
access-list access-list-
number
permit udp source source-
wildcard
host
interface_address_2
eq 69
access-list access-list-
number
remark --- everyone else is
DENIED for TFTP
access
access-list access-list-
number
deny udp any host
interface_address_1
eq 69
access-list access-list-
number
deny udp any host
interface_address_2
eq 69
access-list access-list-
number
remark --- any other traffic
to/through the router
is allowed
access-list access-list-
number
permit ip any any
interface Ethernet0/0
  ip access-group access-list-
number
in

```

Once the tftp server in Cisco IOS is enabled and listening by default on all interfaces enabled for IP processing, the access list would need to deny traffic to each and every IP address assigned to any active router interface.

2. Control Plane Policing: Configure and apply a CoPP policy. For example:

```

access-list access-list-
number
remark --- Do not police TFTP
traffic from trusted
hosts and networks
access-list access-list-
number
deny udp host
source_1 any
eq 69
access-list access-list-
number
deny udp source source-
wildcard
any eq 69
access-list access-list-
number
remark --- Police TFTP traffic
from untrusted
hosts and networks
access-list access-list-

```

```

number
permit udp any any eq
69
access-list access-list-
number
remark --- Do not police any
other traffic going
to the router
access-list access-list-
number
deny ip any any

class-map match-all tftp-
class
  match access-group access-list-
number

policy-map control-plane-
policy
  ! Drop all traffic that matches the class tftp-
class
  class tftp-
class
  drop

control-plane
  service-policy input control-
plane-
policy

```

**Note**

CoPP is only available on certain platforms and Cisco IOS releases. Additional information on the configuration and use of the CoPP feature can be found at the following URL:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml

3. Infrastructure ACLs (iACL) Although often difficult to block traffic transiting your network, identifying traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network is possible. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for iACLs: <http://www.cisco.com/warp/public/707/iacl.html>
4. Configuring Receive Access Lists (rACLs) For distributed platforms, rACLs may be an option starting in Cisco IOS Release 12.0(21)S2 for the Cisco 12000 series GSR and Cisco IOS Release 12.0(24)S for the Cisco 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled “GSR: Receive Access Control Lists” will help identify and allow legitimate traffic to your device and deny all unwanted packets: <http://www.cisco.com/warp/public/707/racl.html>

**Note**

The suggested workarounds are an “all or nothing” solution. While the tftp-server feature in Cisco IOS allows per-file ACLs to be attached to every file being offered for download, the suggested workarounds are global and will either prevent or allow access to all files being shared. It is recommended to apply the suggested workarounds in addition to the existing per-file ACLs, instead of replacing them.

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.

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>

CSCsg16908 IOS FTP Server Deprecation

Symptom This bug documents the deprecation and removal of the Cisco IOS FTP Server feature.

Workaround There is no workaround.

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.

CSCek37177 Malformed tcp packets deplete processor memory.

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

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability. Cisco has made free software available to address this vulnerability for affected customers.

This issue is documented as Cisco bug ID CSCek37177. There are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at:

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

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>

CSCee24395 SYS-3-BADMAGIC after GetNextObjectInstance clogHistoryEntry_get

Symptom A Cisco router may reload if SNMP GetNextObjectInstance request are processed at clogHistoryEntry_get.

Conditions This symptom is observed on a Cisco 7206VXR series router with NPE-300 processor board running IOS 12.2(13)T5.

Workaround The workaround is not to query the CISCO-SYSLOG-MIB. You may create a SNMP view to exclude this MIB and attach this view to all communities configured on the device. This will prevent any managers from accessing the CISCO-SYSLOG-MIB.

CSCsc06695 IKEv1 SA leaks under certain conditions

Symptom When a Phase 1 SA (MM or AM) is being setup and the client does quick retransmissions within a window of one second, the server stops the retransmission timer for the SA. If the client stops retransmissions or further message afterwards, SA on server side is leaked forever (until the lifetime timer expires).

Workaround Clear `isakmp sa` manually.

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>

CSCsb52717 Watchdog timeout and crash caused by invalid MDT data group join packet

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

Conditions Affects all IOS versions that support mVPN MDT.

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

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

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



Note Ensure that the rACL does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering necessary traffic could result in an inability to remotely access the router, thus requiring a console connection. For this reason, lab configurations should mimic the actual deployment as closely as possible.

As always, we recommend that you test this feature in the lab prior to deployment. For more information on rACLs, refer to “*Protecting Your Core: Infrastructure Protection Access Control Lists*” at: <http://www.cisco.com/warp/public/707/racl.html>.

CSCej30903 Enable View Command fails with AAA turned on

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

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

Workaround Configure a method list for the login service.

CSCin95836 NHRP does not handle error conditions gracefully

Symptom A Cisco IOS device configured for NHRP may restart.

Workaround There is no workaround.

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.

Resolved Caveats - Cisco IOS Release 12.3(8)XX2c

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>

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

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

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

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



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

CSCei61732

Symptom 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.

Workaround Cisco has made free software available that includes the additional integrity checks for affected customers. More details can be found in the security advisory which is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

CSCeg15044 You cannot telnet to card.

CSCeh13489 BGP shouldn't propagate updates with AS PATH lengths greater than 255.

CSCed03333

Symptom CBAC sessions are left in sis-closing state due to out-of-order packet handling.

Workaround There is no workaround. But there is a Fix, "Bump out-of-order packets to process path for catch-up, and then drop packets if unsuccessful."

CSCee45312

Symptom 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 to none can be bypassed.

Conditions Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected. Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

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

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

CSCed86842

Symptom Negative Counters are encountered in the Input Queue.

Workaround There is no workaround.

CSCee47441

Symptom When the Cisco IOS Firewall CBAC is configured, the router has a software-forced reload caused by one of the processed inspections.

Conditions 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 There is no workaround.

CSCef44699

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.

Workaround 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>.

CSCef61610

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.

Workaround 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>.

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.

Conditions Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected. Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected. Only devices running certain versions of Cisco IOS are affected.

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

This advisory will be posted at:

http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml.

CSCsa52807

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.

Workaround Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

Resolved Caveats - Cisco IOS Release 12.3(8)XX2D2b

CSCef68324

Symptom Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

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

More details can be found in the security advisory that is posted at:
<http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

Resolved Caveats - Cisco IOS Release 12.3(8)XX2Da

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.

Workaround 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.

Resolved Caveats - Cisco IOS Releases 12.3(8)XX1 and 12.(8)XX2

CSCec88490 Cosmetic Display CLI Related Issues.

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.

Workaround 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>.

CSCee67450

A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (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.

If a malformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

CSCef46191 Unable to telnet.

CSCef56396 IPsec SAs fail to come up for more than one ACL:NAT-T tunnel fails.

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.

Workaround Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources. This advisory is posted at:

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

Additional References

The following sections describe the documentation available for the Cisco 1700 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 IOS Software Documentation Set](#)

Release-Specific Documents

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

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



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>

- 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.

- 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) go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

These documents are available for the Cisco 1700 series routers:

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

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

Cisco IOS Software Documentation Set

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

Documentation Modules

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

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

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

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

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

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

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

