



Release Notes for the Cisco 828 Router for Cisco IOS Release 12.3(2)XC

August 8, 2007
Cisco IOS Release 12.3(2)XC5
OL-8430-02

These release notes describe new features and significant software components for the Cisco 828 router that support Cisco IOS Release 12.3 T, up to and including Cisco IOS Release 12.3(2)XC5. 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 12.3\(2\)T](#) located on [Cisco.com](#).

For a list of the software caveats that apply to Cisco IOS Release 12.3(2)XC5, see the “[Caveats](#)” section on [page 6](#), and refer to the online [Caveats for Cisco IOS Release 12.3\(2\)T](#) document. The caveats document is updated for every 12.3 T maintenance release and is located on [Cisco.com](#).

Contents

These release notes provide information about the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 4](#)
- [Caveats, page 6](#)
- [Additional References, page 35](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 37](#)



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(2)XC 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 Table, page 3](#)

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 12.3(2)XC on the Cisco 828 router.

Table 1 Recommended Memory for the Cisco 828 Router

Platform	Image Name	Feature Set	Image	Flash Memory		DRAM	
				Minimum	Recommended ¹	Minimum	Recommended
Cisco 828	Cisco 828 Series IOS IP	IP	c828-y6-mz	8 MB	8 MB	20 MB	32 MB
	Cisco 828 Series IOS IP/FW	IP/FW	c828-oy6-mz	8 MB	8 MB	20 MB	32 MB
	Cisco 828 Series IOS IP Plus	IP Plus	c828-sy6-mz	8 MB	8 MB	24 MB	32 MB
	Cisco 828 Series IOS IP/FW Plus 3DES	IP/FW Plus 3DES	c828-k9osy6-mz	8 MB	8 MB	32 MB	32 MB

1. Recommended memory is the memory required considering future expansions.

Hardware Supported

Cisco IOS Release 12.3(2)XC supports the following router:

- Cisco 828 router

For detailed descriptions of new hardware features and which features are supported on each router, see the “[New and Changed Information](#)” section on page 4. 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 828 router, which are available on [Cisco.com](#) at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/800/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:

Cisco Product Documentation: Access Servers and Access Routers: Fixed Access: Cisco 800 Series Routers: <platform_name>

Determining the Software Version

To determine which version of the Cisco IOS software is currently running on your Cisco 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 on the second output line.

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C836 Software (C836-K9O3SY6-M), Version 12.3(2)XC4, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.3(1.6)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 Table

Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Cisco IOS Release 12.3(2)XC includes new features that are supported by the Cisco 828 router. Cisco IOS Release 12.3(2)XC54 includes the same feature sets as Cisco IOS Releases 12.3, 12.3(2)T, and 12.3(2)XC.



Caution

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 due to 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](#) lists the features and feature sets that are supported in Cisco IOS Release 12.3(2)XC.

The table uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, “12.3(2)XC” indicates that the feature was introduced in Cisco IOS Release 12.3(2)XC. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.

**Note**

This feature set table contains only a selected list of features, which are cumulative for Release 12.3(2)*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 the *Cross-Platform Release Notes for Cisco IOS Release 12.3(2)T* and Release 12.3 T Cisco IOS documentation.

Table 2 Feature Set Table for the Cisco 828 Router

Feature	In	Feature Set			IP/FW Plus 3DES
		IP	IP FW	IP Plus	
TACACS+		Yes	Yes	Yes	Yes
Class-Based Traffic Policing with CLP Tagging	12.3(2)XC	No	No	Yes	Yes
URPF	12.3(2)XC	Yes	Yes	Yes	Yes
DNS Proxy		Yes	Yes	Yes	Yes

New and Changed Information

The following sections list the new information about the Cisco 828 router for Cisco IOS Release 12.3(2)XC and Release 12.3(2)T. Cisco IOS Release 12.3(2)XC supports the features listed in this section.

New Software Features in Cisco IOS Release 12.3(2)XC

The following sections describe the new software features supported by the Cisco 828 router for Cisco IOS Release 12.3(2)XC:

TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a Unix or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting (AAA) facilities.

For more details, refer TACACS+ technical documentation located at the following URL:

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

Class-Based Traffic Policing with CLP Tagging

When configured on the router Class-Based Traffic Policing with Cell Loss Priority (CLP) Tagging polices the flow of cells in the forward (into the network) direction of a virtual connection. The traffic policing mechanism determines whether received cells comply with the negotiated traffic management values and tag the cell with a CLP bit value of 1. The purpose of this feature is to mark traffic that does not meet the traffic management values so that packets that exceed the set values can be dropped by the network if the network is congested.

For more details on Class-Based Policing, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s26/fspolic.htm>

For more details on CLP Tagging, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt1/qcfcbmrk.htm

Unicast Reverse Path Forwarding

The Unicast Reverse Path Forwarding (URPF) feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribe Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.

For more details on how to configure URPF, refer to the following URLs:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/secure.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/122sy/cmdref/i1.htm>

DNS Proxy

In virtual private network (VPN), Point-to-Point Protocol over Ethernet (PPPOE), etc. PCs connected to the LAN may get Dynamic Host Configuration Protocol (DHCP) parameters including the IP addresses of the Domain Name System (DNS) server prior to the router connecting to the WAN to get the information over IP Control Protocol (IPCP). The objective with Proxy DNS (or caching-only name server) enables the router to receive DNS queries on behalf of the real DNS servers and proxy for the hosts on the LAN connected users. This enables the DHCP server to immediately send the hosts the router's own LAN address in lieu of the DNS server's IP address. The router forwards the DNS queries from local users to real DNS servers after the WAN connection comes up and caches the DNS records in response. Over the time, cache includes the DNS information most often requested by the local resolvers and this can reduce the overhead of packets to the WAN.

The router must obtain the correct DNS server information from the WAN in order for it to function as a proxy DNS server.

The global configuration command **ip dns server** enables DNS proxy server functionality on the router, and causes it to forward DNS queries to the actual DNS servers. The global configuration command **dns-server address** causes the router to respond to DNS queries with its own IP address.

New Software Features in Cisco IOS Release 12.3(2)T

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

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/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 T)

Caveats

Caveats describe unexpected behavior or defects in 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 Release 12.3 T are also in Cisco IOS Release 12.3(2)XC. For information on caveats in Cisco IOS Release 12.3 T, refer to the *Caveats for Cisco IOS Release 12.3(2)T* document. This document lists severity 1 and 2 caveats; the documents are 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.

- [Resolved Caveats - Cisco IOS Release 12.3\(2\)XC5, page 7](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(2\)XC4, page 25](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(2\)XC3, page 26](#)
- [Resolved Caveats - Cisco IOS Release 12.2\(2\)XC2, page 32](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(2\)XC1, page 33](#)
- [Resolved Caveats - Cisco IOS Release 12.3\(2\)XC, page 34](#)
- [Open Caveats - Cisco IOS Release 12.3\(2\)XC, page 35](#)

Resolved Caveats - Cisco IOS Release 12.3(2)XC5

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-snmv3.shtml>

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

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

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

For example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                        00000000011111111111222222222333^
                        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 caused other locations in memory to be corrupted.

CSCeb56909 Crafted packet causes reload on Cisco routers

Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

More details can be found in the security advisory which is posted at

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

CSCec16481 Software forced crash when router receives corrupted OSPF Hello

A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml>

CSCec71950 Crafted IP Option may cause DoS or code execution

Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

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 vulnerability was discovered during internal testing.

This advisory is available at:

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

CSCed26739 mm/gk/gk_cli.c:CLI:gw-type-prefix possible buffer overflow

Symptom The router will reload if "sh run" is given after a tech-prefix terminating with a large number of '.'s is configured as follows.

```
conf t
  gatekeeper
    gw-type-prefix 1234.....
```

Conditions

```
conf t
  gatekeeper
    gw-type-prefix
      1234.....

and enter command sh run
```

Workaround Do not enter long tech-prefix and using the "....." pattern

CSCed27956 TCP checks should verify ack sequence number

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

CSCed38527 TCP checks should verify syn sequence number

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

CSCed40933 Multiple crafted IPv6 packets cause reload

Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

More details can be found in the security advisory which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.

`CSCed68575 Reload triggered in SNMP process`

Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with [CSCed68575](#).

This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml>

`CSCed93836 modifications needed to syn rst packet response`

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the

application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

`CSCee08584 ITS/CME: aberrant data may trigger reload`

Cisco Internetwork Operating System (IOS®) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for the Cisco IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.

A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml>

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

This vulnerability is documented by Cisco bug ID [CSCee08584](#).

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.

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>

CSCef46191 Unable to telnet

Symptom 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.

Conditions User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

Workaround The detail advisory is available at
<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

CSCef48336 Corrupted OSPF Hello packets caused software forced crash

Symptom 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>

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>

CSCef77013 tighter parameter checking for ipv6

Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected 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>.

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>

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>

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>

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>

CSCin95836 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>.

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

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>

CSCsb12598 Router forced crash on receiving fragmented TLS ClientHello

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

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

Cisco IOS is affected by the following vulnerabilities:

- * Processing ClientHello messages, documented as Cisco bug ID [CSCsb12598](#)
- * Processing ChangeCipherSpec messages, documented as Cisco bug ID [CSCsb40304](#)
- * Processing Finished messages, documented as Cisco bug ID [CSCsd92405](#)

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

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



Note

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

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

CSCsb33172 short-circuit crypto engine operations when faking AM2

Symptom 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>

CSCsb40304 Router crash on sending repetitive SSL ChangeCipherSpec

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

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

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID [CSCsb12598](#)
- Processing ChangeCipherSpec messages, documented as Cisco bug ID [CSCsb40304](#)
- Processing Finished messages, documented as Cisco bug ID [CSCsd92405](#)

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

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



Note

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

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

CSCsb79076 MGCP RSVP enabled calls fails due to spurious error @ qosmodule_main

Symptom [%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.

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/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900ae cd804fa16a.html.

CSCsc60249 Crash while processing malformed SIP packet

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

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

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

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

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

CSCsc64976 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>

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.

CSCsd81407 Router crash on receiving abnormal MGCP messages

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

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

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

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

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

CSCsd85587 7200 Router crashes with ISAKMP Codenomicon test suite

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

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

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

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

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

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

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

CSCsd92405 router crashed by repeated SSL connection with malformed finished message

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

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

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID [CSCsb12598](#)
- Processing ChangeCipherSpec messages, documented as Cisco bug ID [CSCsb40304](#)
- Processing Finished messages, documented as Cisco bug ID [CSCsd92405](#)

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



Note

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

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

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

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

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.

CSCse56501

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

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

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

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>

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.

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

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

CSCsf07847 cdp may fail to discover neighbor information in releases wh CSCse85200

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

Conditions When the cdp packet header length is lesser than predefined header length(4 bytes).

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

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>

CSCsg03449 Etherswitch module VLAN Trunking Protocol Vulnerabilities

- 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:

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>

CSCsg16908 IOS FTP Server Deprecation

Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's file system, 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>.

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.

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>

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 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>

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.

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.

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.

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.

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.



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>

Resolved Caveats - Cisco IOS Release 12.3(2)XC4

- CSCeb85136—IP packets sent with invalid checksums are not discarded.

Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value.

Workaround: There is no workaround.
- 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>.
- CSCee77121—Router crashes when 10th AAL2 PVC is created in the ATM Interface.
- CSCeg15044—Not able to telnet to card (No Free TTYs error).
- CSCeg47738—An incorrect count is loaded into the Timer3 that handles ISDN layer1.
- CSCeh13489—BGP shouldn't propagate updates with AS Path lengths greater than 255.
- CSCeh47763—NAT cause router to generate ACKs for RSTs of non-local tcp session.

Symptoms: Router may erroneously send ACK packets in response to RST packets for non-local TCP sessions. This can cause high CPU utilization on the router.

Conditions: This symptom occurs when using Port Address Translation (PAT).

Workaround: Use the **clear ip nat translation *** command.
- 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>.
- CSCsa52807—L2TP 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 [National Infrastructure Security Coordination Centre](#).

- 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

Resolved Caveats - Cisco IOS Release 12.3(2)XC3

- CSCdz32659—%SYS-2-MALLOCFAIL: -Process= CDP Protocol.

Memory allocation failure (MALLOCFAIL) messages may occur for a Cisco Discovery Protocol (CDP) process:

```
%SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
Processor, alignment 0
```

```
-Process= "CDP Protocol", ipl= 0, pid= 42
```

```
-Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
```

Workaround: To prevent the symptom from occurring again, disable CDP by entering the **no cdp run** global configuration command.

- CSCdz84583—Cisco IOS fw allows forged packets for a session initiated from inside.

A vulnerability in the TCP specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a

router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, the attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability. An advisory that describes this vulnerability for products that run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>. A companion advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOS software.

- CSCeb16876—Bad getbuffer, crash, tag input, fragmentation.

The router may generate a “SYS-2-GETBUF” message during the “Tag Input” process and may subsequently reload unexpectedly. This symptom is observed when the router fragments a MultiProtocol Label Switching (MPLS) packet.

Workaround: None.

- CSCeb52066—NAT: Provide an API to get the pre-natted TCP Seq/Ack Numbers.

A vulnerability in the TCP specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, the attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability. An advisory that describes this vulnerability for products that run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>. A companion advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOS software.

- CSCeb56909—Crafted packet causes reload on Cisco routers.

Routers running Cisco IOS software that supports MPLS are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

More details can be found in the security advisory which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>.

- CSCeb88239—const2:crash RIPv6_input after sending 1 packet to FF02::9 M/cast Ad.

A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a DoS on the device. This symptom is observed when the **ipv6 debug rip** command is enabled on the router. Malformed packets can normally be sent locally. However, when the **ipv6 debug rip** command is enabled, the crash can also be triggered remotely. Note that RIP for IPv4 is not affected by this vulnerability.

Workaround: None.

- CSCec16481—Software-forced crash when router receives corrupted OSPF Hello.

A device running Cisco IOS and enabled for the OSPF Protocol is vulnerable to a DoS attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml>.

- CSCec25430—Cisco IOS may reload from specific packet.
A Cisco device reloads on receipt of a corrupt CDP packet. This symptom is observed when an empty “version” field exists in the output of the **show cdp entry *** command for at least one entry. One possible scenario is:
Reloading a faulty Cisco IP conference station 7935 or 7936 may cause a connected Cisco switch or router to reload. A CDP message may appear on the terminal, such as the following one:
%CDP-4-DUPLEX_MISMATCH duplex mismatch discovered on FastEthernet5/1 (not half duplex), with SEP00e0752447b2 port 1 (half duplex).
Workaround: Disable CDP by entering the **no cdp run** global configuration command.
First Alternate Workaround: Disable CDP on the specific (sub-)interface(s) whose corresponding neighbor(s) has or have an empty “version” field in the output of the **show cdp entry *** command.
Second Alternate Workaround: Disconnect the 7935 or 7936 phone, in the case of the specific symptom that is described above.
- CSCec59206—Bus error in nat translating RSHELL packets.
A router may reload unexpectedly because of a bus error when it accesses a low address during the translation of TCP port 514. This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(5) and that is configured for Network Address Translation (NAT).
Workaround: Prevent the translation of TCP port 514.
- CSCec86420—Undebug All stops traffic with IPsec+GRE+CEF (also see CSCeb56909).
Routers running Cisco IOS software that supports MPLS are vulnerable to a DoS attack on MPLS disabled interfaces. This is a complementary fix to CSCeb56909 which addresses this vulnerability.
More details can be found in the security advisory which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>.
- 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.
- CSCed35253—Router may crash due to corrupted data in list with Cisco IOS-firewall.
A router may reload unexpectedly after it attempts to access a low memory address. This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.
Workaround: Disable IP Inspect and IDS.
- CSCed40563—Malicious cfg reload neighbor routers by **show cdp entry * protocol**.
Depending upon configuration, issuing the **show cdp entry * protocol** command may cause a reload of the device. This symptom occurs on Cisco products that are speaking CDP with configurable interface MTU.
Workaround: Disable CDP, avoid issuing the command under given circumstances, or upgrade to a fixed version of software.
- CSCed40933—Multiple crafted IPv6 packets cause reload.

Cisco IOS software is vulnerable to a DoS attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation. More details can be found in the Security Advisory which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.

- CSCed68575—Reload triggered in SNMP process.

Cisco IOS software release 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload. The vulnerability is only present in certain Cisco IOS releases on routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575. This vulnerability can be remotely triggered. A successful exploitation of the vulnerability may cause a reload of the device and could be exploited repeatedly to produce a DoS. For more information, please see the advisory available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmpl.shtml>.

- CSCed78149—TCP connections doing PMTU discovery vulnerable to spoofed ICMP packets.

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 [National Infrastructure Security Coordination Centre](#).

- CSCed93836—Modifications needed to syn rst packet response.

A vulnerability in the TCP specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability. An advisory that describes this vulnerability for products that run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>. A companion advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOS software.

- CSCee08584—ITS/CME: aberrant data may trigger reload.

When configured for the Cisco IOS Telephony Service (ITS), Cisco CallManager Express (CME), or Survivable Remote Site Telephony (SRST), Cisco IOS release 12.3 T may contain a vulnerability in processing certain malformed control protocol messages. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a DoS.

Cisco has made free software upgrades available to address this vulnerability for all affected customers. There are workarounds available to mitigate the effects of the vulnerability. Please see the advisory available at <http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml>.

- 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>.

- CSCef43691—L2TPv3 and UTI sessions doing PMTUD vulnerable to spoofed ICMP packets.

See note for CSCed78149.

- CSCef44225—IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets.

See note for CSCed78149.

- CSCef44699—GRE and IPinIP doing PMTUD vulnerable to spoofed ICMP packets.

See note for CSCed78149.

- CSCef46191—Unable to telnet.

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

User-initiated, specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions, however, services such as packet forwarding, routing protocols, and all other communication to and through the device remain unaffected.

Please see the advisory available at

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

- CSCef60659—More stringent checks required for ICMP unreachable.
See note for CSCed78149.
- CSCef61610—Incorrect handling of ICMPv6 messages can cause TCP performance problems.
See note for CSCed78149.
- CSCef67682
Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

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

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

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

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

We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml> contain fixes for this issue.

- 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.
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.
- CSCin67568—Memory leak in CDP process with long host names.
A Cisco device experiences a memory leak in the CDP process when the device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.
Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the global command **no cdp run**.
- CSCin82407—XAUTH failure and blank ACK can allow Phase 2 negotiation.
Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.
Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to

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

- CSCsa59600—IPSec PMTUD not working [after CSCef44225].
See note for CSCed78149.
- CSCsa61864—Enhancements to L2TPv3 PMTUD may not work [follow-up to CSCef43691]
See note for CSCed78149.

Resolved Caveats - Cisco IOS Release 12.2(2)XC2

- CSCec00345—Adjustments of tones in accordance with Spanish and ITU-T standards.
When Phone1 goes on hook and Phone2 stays up after the conversation is over, user on Phone2 can hear the OFFHOOK_NOTICE which is not defined in ITU-T E.180 or in National Spanish standards.
Workaround: Define the custom tone table.
- CSCed27956—TCP checks should verify ack sequence number.
A vulnerability in the TCP specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.
All Cisco products which contain a TCP stack are susceptible to this vulnerability. An advisory that describes this vulnerability for products that run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>. A companion advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOS software.
- CSCed34050—Cisco 837 router: Middle buffers and HIFN79xx buffers issues.
A Cisco 837 router may encounter memory allocation failures in I/O memory.
Workaround: None.
- CSCed38527—TCP checks should verify syn sequence number.
A vulnerability in the TCP specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain a TCP stack are susceptible to this vulnerability. An advisory that describes this vulnerability for products that run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>. A companion advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOS software.

- CSCed50319—Enable **ip qos dscp** CLI in base images of Cisco 820 router.
- CSCed50556—Memory leak in Crypto IKMP.

The memory that Crypto Internet Key Management Protocol (IKMP) process holds increases. That memory is not freed and after some time may take all the memory.

Workaround: None.

- CSCed76042—Adding Policy-Based Routing (PBR) support for Cisco SOHO 97 router.

Resolved Caveats - Cisco IOS Release 12.3(2)XC1

- CSCdz27562—**snmpwalk** on loopbacks gets no response.

Executing an **snmpwalk** command on loopback interface does not yield any results.

Workaround: Execute the **snmpwalk** command on the physical interface.

- CSCeb22276—Delay in processing some SNMP requests.

Some SNMP packets may stay in the input queue while being processed. However, the packets do drain on their own without any intervention from the user. This fix allows those packets to be removed from the queue more quickly.

Workaround: Protect your SNMP community strings with good password management. Permit SNMP traffic only from trusted devices.

- CSCeb70171—MPLS-QoS: Spurious memory access occurs with MLPPPoFR and WRED.

An alignment traceback may occur when a router is configured for Multilink PPP over Frame Relay (MLPoFR) and weighted random early detection (WRED).

Workaround: Remove or modify the service-policy map to prevent WRED from running on MLPPPoFR interfaces.

- CSCeb79675—SNMP reply packets do not use the correct source address.

A SNMP request sent to the loopback interface of a Cisco router will have the wrong source address in the reply.

Workaround: Send the SNMP request to the IP address of a physical interface.

- CSCec00345—Adjustments of tones in accordance with Spanish and ITU-T standards.

When the phone connected to FXS port of the Cisco 827-4V router goes on hook, the receiver on the other end can hear off hook notice. This is not defined in ITU-T E.180 or in National Spanish standards.

Workaround: Define the custom tone table.

- CSCec36893—Multiple PPPoE client sessions are not created.

When multiple **pppoe-client** and **dial-pool-number** commands are configured on the interface, only one session is created after reloading the router.

Workaround: None.

- CSCec77078—Packet delay over IPSec tunnel when HW crypto used.
Workaround: Disable hardware encryption with **no crypto engine accelerator** command.
- CSCed00310—Managed Switch: Backout CSCeb45932 to go for advertisement setting.
- CSCed02145—Caller ID in Spain not working on all phones.
Some phones that display caller ID on the PSTN in Spain do not display caller ID on Foreign Exchange Station (FXS) ports on the Cisco 827 router.

Resolved Caveats - Cisco IOS Release 12.3(2)XC

- CSCea64214—Potential scalability issue with dot1x and Windows 2000 client.
- CSCea78615—Software forced crash at “mgd_timer_first_running” related to Next Hop Resolution Protocol (NHRP).
The Cisco router running NHRP may reload due to a software forced crash.
Workaround: None.
- CSCea90932—SIP call does not go through when port 1024 is used in Via header.
Workaround: Attempt another call. Call works when port number in Via header is greater than 1024.
- CSCeb08445—Default route learned via DHCP overrides static default route.
Workaround: Configure the command **ip dhcp-client default-router distance** to be the same as the statically configured route distance. This way, the DHCP learned route will overwrite the configured route but with the same information.
- CSCeb41084—Routing loop issue with DHCP and Dynamic Multipoint VPN (DMVPN).
- CSCeb42787—DHCP static routes are not being removed.
Workaround: After configuration change, save the configuration, and reload the router.
- CSCeb44999—CNS configuration notify extensible markup language (XML) output needs to handle control and carriage return characters.
Workaround: None.
- CSCeb45670—Multi-line banner command is not correctly applied by CNS configuration agent.
Workaround: None.
- CSCeb46738—If VPN group is not cleared immediately, it leads to invalid attribute reuse.
Workaround: Wait till all the Internet Security Association and Key Management Protocol (ISAKMP) security association table is flushed and try again. The tunnel will not come up and it will show an error.
- CSCeb56827—When of Easy VPN client is rebooted, unknown transform error is displayed.
Workaround: Disable VPN card, or remove and re-apply the crypto map from the interface.
- CSCeb71671—NHRP on multi-point generic routing encapsulation (GRE) tunnel interface causes router to crash.
Workaround: None.
- CSCeb87159—CNS sends keepalive values to tibgate incorrectly.
Workaround: None.

- CSCec03928—Cannot see running configuration when Cisco Networking Services (CNS) configuration is downloaded.
Workaround: Hook-up the console.
- CSCec06005—Memory leaks in NHRP and tunnel protection.
- CSCec15351—CNS configuration agent modifies the configuration without persisting it.
Workaround: Ensure there is no concurrent access to the router.
- CSCec25744—IOS image reloads when connecting spoke to spoke.
Workaround: Disable all spoke-to-spoke connections.
- CSCcuk43613—CNS syntax checker fails on **encapsulation aal5snap** command.
Workaround: Disable the syntax checker when trying to apply configuration with the **encapsulation aal5snap** command.

Open Caveats - Cisco IOS Release 12.3(2)XC

- CSCeb87091—The Cisco 7200 series router will not perform BGP update in PPPoE with IP CEF enabled.
Workaround: Disable IP CEF on the dialer interface by using the command **no ip route-cache cef**.
- CSCin52746—PBR does not work for two policy set under route-map.
- CSCin56511—PPPoE client does not send PPPoE Active Discovery Terminate when **clear/shutdown** commands are given on dialer interface.

Additional References

The following sections describe the documentation available for the Cisco 828 router. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration 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 in pdf or html form.

Use these release notes with the documents listed in the following sections:

- [Release-Specific Documents, page 35](#)
- [Platform-Specific Documents, page 36](#)

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.3(2)XC5. They are located on [Cisco.com](#):

- *Cross-Platform Release Notes for Cisco IOS Release 12.3T*
- *Field Notices:* http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- *Caveats for Cisco IOS Release 12.3 and Caveats for Cisco IOS Release 12.3T*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 828 router are available on [Cisco.com](http://www.cisco.com) at the following location:

http://www.cisco.com/en/US/products/hw/routers/tsd_products_support_category_home.html

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.3 and Cisco IOS Release 12.3(2)XC, and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only.

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Cisco Feature Navigator is available 24 hours a day, 7 days a week.

To use Cisco Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Cisco Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/cfn>

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