Release Notes for the Cisco SOHO 70 Series and Cisco 820 Series Routers for Cisco IOS Release 12.2(13)ZH

November 16, 2007
Cisco IOS Release 12.2(13)ZH10
OL-4160-03

These release notes describe new features and significant software components for the Cisco SOHO 71, SOHO 76, SOHO 77, and the Cisco 826, Cisco 827, and Cisco 828 routers that support Cisco IOS Release 12.2 T, up to and including Cisco IOS Release 12.2(13)ZH. 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 12.2 T* located on Cisco.com.

For a list of the software caveats that apply to Cisco IOS Release 12.2(13)ZH, see the "Caveats" section on page 8, and refer to the online *Caveats for Cisco IOS Release 12.2 T* document. The caveats document is updated for every 12.2 T maintenance release and is located on Cisco.com.

Contents

These release notes provide information about the following topics:

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

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(13)ZH and includes the following sections:

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Cisco IOS Release 12.2(13)ZH8 on the Cisco SOHO 70 series and Cisco 820 series routers.

Table 1 Recommended Memory for the Cisco SOHO 70 Series and Cisco 820 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco SOHO 71	Cisco SOHO 71Series IOS IP/FW	IP/FW	soho71-oy6-mz	8 MB	16 MB
Cisco SOHO 76	Cisco SOHO 76 Series IOS IP/FW	IP/FW	soho70-oy1-mz	8 MB	16 MB
	Cisco SOHO 76 Series IOS IP	IP	soho70-y1-mz	8 MB	16 MB
Cisco SOHO 77	Cisco SOHO 77 Series IOS IP/FW	IP/FW	soho70-oy1-mz	8 MB	16 MB
	Cisco SOHO 77 Series IOS IP	IP	soho70-y1-mz	8 MB	16 MB
Cisco SOHO 77H	Cisco SOHO 77 Series IOS IP/FW	IP/FW	soho70-oy1-mz	8 MB	16 MB
Cisco 826	Cisco 826 Series IOS IP	IP	c820-y6-mz	8 MB	20 MB
	Cisco 826 Series IOS IP Plus	IP Plus	c820-sy6-mz	8 MB	24 MB
	Cisco 826 Series IOS IP/FW	IP /FW	c820-oy6-mz	8 MB	20 MB
	Cisco 826 Series IOS IP/FW Plus IPSec 3DES	IP/FW Plus/ IPSec 3DES	c820-k9osy6-mz	8 MB	24 MB
Cisco 827	Cisco 827 Series IOS IP	IP	c820-y6-mz	8 MB	20 MB
	Cisco 827 Series IOS IP Plus	IP Plus	c820-sy6-mz	8 MB	24 MB
	Cisco 827 Series IOS IP/FW	IP /FW	c820-oy6-mz	8 MB	20 MB
	Cisco 827 Series IOS IP/FW Plus IPSec 3DES	IP/FW Plus/ IPSec 3DES	c820-k9osy6-mz	8 MB	24 MB
Cisco 827H	Cisco 827H Series IOS IP	IP	c820-y6-mz	8 MB	20 MB
	Cisco 827H Series IOS IP Plus	IP Plus	c820-sy6-mz	8 MB	24 MB
	Cisco 827H Series IOS IP/FW	IP /FW	c820-oy6-mz	8 MB	20 MB
	Cisco 827H Series IOS IP/FW Plus IPSec 3DES	IP/FW Plus/ IPSec 3DES	c820-k9osy6-mz	8 MB	24 MB

Table 1 Recommended Memory for the Cisco SOHO 70 Series and Cisco 820 Series Routers (continued)

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 827-4V	Cisco 827-4V Series IOS IP/Voice	IP/Voice	c820-v6y6-mz	8 MB	32 MB
	Cisco 827-4V Series IOS IP/Voice Plus	IP/Voice Plus	c820-sv6y6-mz	8 MB	32 MB
	Cisco 827-4V Series IOS IP/FW/Voice	IP /FW/Voice	c820-ov6y6-mz	8 MB	32 MB
	Cisco 827-4V Series IOS IP/FW/Voice Plus 3DES	IP/FW/Voice Plus/ 3DES	c820-k9osv6y6-mz	8 MB	32 MB
Cisco 828	Cisco 828 Series IOS IP	IP	c828-y6-mz	8 MB	20 MB
	Cisco 828 Series IOS IP Plus	IP Plus	c828-sy6-mz	8 MB	20 MB
	Cisco 828 Series IOS IP/FW	IF/FW	c828-oy6-mz	8 MB	20 MB
	Cisco 828 Series IOS IP/FW Plus IPSec 3 DES	IP/FW Plus/ IPSec 3DES	c828-k9osy6-mz	8 MB	24 MB

Hardware Supported

Cisco IOS Cisco IOS Release 12.2(13)ZH8 supports the following routers:

- Cisco SOHO 71 router
- Cisco SOHO 76 router
- Cisco SOHO 77 router
- Cisco SOHO 77H router
- Cisco 826 router
- Cisco 827 router
- Cisco 827-4V router
- Cisco 827H 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 5. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to these routers, 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 12.2(13)ZH8, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.2(14.5)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see the *Software Installation and Upgrade Procedures*, which are located at http://www.cisco.com/warp/public/130/upgrade_index.shtml.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Cisco IOS Release 12.2(13)ZH supports the same feature sets as Releases 12.2 and 12.2(13)T, but Cisco IOS Release 12.2(13)ZH also includes new features. Cisco IOS Release 12.2(13)ZH9 is a rebuild of Cisco IOS Release 12.2(13)ZH and includes only bug fixes, it does not include any new features.

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 Cisco IOS Release 12.2(13)ZH.

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, "12.2(13)ZH" indicates that the feature was introduced in 12.2(13)ZH. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.

Note These feature set tables contain only a selected list of features, which are cumulative for Release 12.2(13)*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 12.2 T* and Release 12.2 T Cisco IOS documentation.

Table 2 Feature List by Feature Set

Feature	In	Feature Set		
		IP/FW/IPSec 3DES	IP Plus/ FW/IPSec 3DES	IP Plus/FW/ Dial Backup IPSec 3DES
FTP/Telnet Authentication Proxy	12.2(13)ZH	Yes	Yes	Yes
URL Filtering—Websense	12.2(13)ZH	No	Yes	Yes
URL Filtering—N2H2	12.2(13)ZH	No	Yes	Yes
SIP Through Firewall	12.2(13)ZH	Yes	Yes	Yes
CBQoS MIB and DSCP	12.2(13)ZH	No	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	12.2(13)ZH	Yes	Yes	Yes
Direct HTTP Enroll with CA Servers	12.2(13)ZH	Yes	Yes	Yes

New and Changed Information

The following sections list the new information for Cisco IOS Release 12.2(13)ZH. This information also applies to Cisco IOS Release 12.2(13)ZH8.

New Software Features in Release 12.2(13)ZH

The following sections describe the new software features for Cisco IOS Release 12.2(13)ZH.

FTP/Telnet Authentication Proxy

The authentication proxy in the Cisco IOS firewall feature set currently supports only HTTP protocol. Authentication Proxy support has been extended to FTP/Telnet protocols with this release. This release also introduces absolute timeout functionality to the authentication proxy feature. The absolute timeout sets a time window during which the authentication proxy on the enabled interface is active. As the absolute timer expires, the authentication proxy will be disabled. The addition of the absolute timeout upgrades the functionality of the authentication proxy and also meets the firewall requirements.

Example

The following configuration example shows how to enable authentication proxy on FTP/Telnet application using Tacacs+ as the AAA server.

```
!
aaa new-model
!
!
aaa authorization exec default group tacacs+
aaa authorization network default group tacacs+
aaa authorization auth-proxy default group tacacs+
!
ip inspect name ftp-telnet ftp timeout 55
ip inspect name ftp-telnet tcp timeout 55
ip auth-proxy auth-proxy-audit
ip auth-proxy name pxy telnet
```

```
ip auth-proxy name pxy ftp
ip auth-proxy inactivity-timer 1
ip auth-proxy absolute-timer 1
!
interface Ethernet0
ip address 192.168.8.2 255.255.255.0
ip access-group 105 in
ip inspect ftp-telnet in
ip auth-proxy pxy
!
access-list 105 deny   udp any any
access-list 105 permit tcp any any
access-list 105 permit ip any any
!
tacacs-server host 192.168.2.19 port 9000
tacacs-server directed-request
tacacs-server key cisco
!
```

URL Filtering—Websense

Websense is a third-party URL filtering software program that can filter HTTP requests, based on destination host name, destination IP address, keywords, and username. Websense maintains a URL database of more than 20 million sites organized into more than 60 categories and subcategories. This feature enables the Cisco IOS firewall to do URL filtering based on Websense server. When a Cisco 800 router receives an HTTP request, it sends a query request to the Websense server with the requested URL. The Websense server does some necessary lookups for the URL and sends back a query response. Based on the Websense server's response, the router either blocks the HTTP request by redirecting the browser to a block page or proceeds with normal HTTP processing.

For more information on this feature, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftwebsen.html

URL Filtering—N2H2

N2H2 is globally deployed third-party URL filtering software that can filter HTTP requests, based on destination host name, destination IP address, username, and password. It relies on a sophisticated URL database of more than 15 million sites organized into more than 40 categories using both Internet technology and human review. This feature enables the Cisco IOS firewall to do URL filtering based on N2H2 server. When a Cisco 800 router receives an HTTP request, it sends a query request to N2H2 server with the requested URL. N2H2 server does some necessary lookups for the URL and sends back a query response. Based on N2H2 server's response, the router either blocks the HTTP request by redirecting the browser to a block page or proceeds with normal HTTP processing.

For more information on this feature, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_fwall_n2h2_supp_external_docbase_0900e4b1805afe39_4container_external_docbase_0900e4b1807afcc8.html

SIP Through Firewall

This feature allows Session Initiation Protocol (SIP) signaling requests to traverse directly between gateways or through a series of proxies to the destination gateway or phone. After the initial request, if the Record-Route header field is not used, subsequent requests can traverse directly to the destination gateway address as specified in the Contact header field. Thus, the Cisco IOS firewall is aware of all surrounding proxies and gateways and allows the following functionality:

- SIP signaling responses can travel the same path as SIP signaling requests.
- Subsequent signaling requests can travel directly to the endpoint (destination gateway).
- Media endpoints can exchange data.

For more information on this feature, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_fwsip.html

CBQoS MIB and DSCP

The Class-Based Quality of Service Management Information Base (CBQoS MIB) provides access to quality of service (QoS) configuration information and statistics. The CBQoS MIB allows service providers to monitor their QoS offerings. This MIB gives QoS configuration done in the router such as ClassMap, PolicyMap, Match Statements and Feature Actions configuration parameters. The MIB also contains counter objects which gives statistics information such as the number of packets traversed conforming to a policing feature. The MIB uses several indexes to identify QoS features and to distinguish among instances of those features. The MIB provides information about marking and policing done using IP precedence and Differentiated Services Code Point (DSCP).

Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy Protocol (VRRP) feature can solve the static configuration problem. VRRP enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

VRRP is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, and on MPLS VPNs and VLANs.

For more details on this feature, refer to the following URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_tech_note09186a0080094490.shtml

Direct HTTP Enroll with CA Servers

Some Certificate Authorities (CA) support enrollment via HTTP. The Cisco IOS allows a user to specify a profile for HTTP enrollment related operations. The Cisco IOS will fill in the command template within the profile with the PKCS 10 certificate request and up to eight user provided values. The resulting message will be sent to the HTTP server and the response will be parsed for a PEM format certificate.

For more details of this feature, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gthttpca.html

New Software Features in Release 12.2T

For information regarding the features supported in Cisco IOS Release 12.2 T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/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:

Service & Support: **Technical Documents**: **Cisco IOS Software**: **Release 12.2**: **Release Notes**: **Cross-Platform Release Notes** (Cisco IOS Release 12.2 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 12.2 T are also in Cisco IOS Release 12.2(13)ZH. For information on caveats in Cisco IOS Release 12.2 T, refer to the *Caveats for Cisco IOS Release 12.2 T* document. For information on caveats in Cisco IOS Release 12.2, refer to the *Caveats for Cisco IOS Release 12.2* document. These documents list severity 1 and 2 caveats; the documents are located on Cisco.com.

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com, and 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- Release 12.2(13)ZH10

`CSCsb79076 MGCP RSVP enabled calls fails due to spurious error`

Symptom %SYS-3-TIMERNEG errors and tracebacks are observed while making MGCP RSVP calls on analog (RGW) setups.

Conditions This issue is observed in 12.4(3.9)T1 IOS version.

Workaround There is no workaround.

`CSCsj18014 Caller ID string received with extra characters`

Symptom Caller ID is received with extra characters.

Conditions The condition is that whatever name that was sent by the source, will be received in the destination.

Workaround There is no workaround.

CSCef61610 Incorrect handling of ICMPv6 messages can cause TCP performance problems

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt). These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages

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

3. Attacks that use ICMP "source quench" messages Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft. Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

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

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

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

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

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

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

CSCef48336 Corrupted OSPF Hello packets caused software forced crash

OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89. If an 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 Use 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/en/US/tech/tk365/technologies_configuration_example09186a0080094069.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

CSCec16481 Software forced crash when router receives corrupted OSPF Hello

Symptom 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.

Workaround Further details and the workaround 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

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

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 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.

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

CSCee45312 Radius authentication bypass when configured with a none fallback method

Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed. Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected.

Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

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

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

CSCei61732 Additional Data Check in System Timer

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

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

CSCef68324 ICMPv6 pkt traceback

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

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

http://www.cisco.com/en/US/products/products_security_advisory09186a00804d82c9.shtml

CSCsj16292 DATACORRUPTION-1-DATAINCONSISTENCY: copy error

Symptom Following an upgrade to 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 this does not impact the service.

Workaround There is no workaround.

CSCsg70355 PWE3:%DATACORRUPTION-1-DATAINCONSISTENCY: copy error

CSCeb21064 Crash while processing malformed SIP packet

Symptom 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.

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

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

CSCse68138 Issue in handling specific packets in VOIP RTP Lib

Symptom 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.

Workaround 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 behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

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

Workaround Disable the interfaces where CDP is not necessary.

`CSCsc60249 Crash while processing malformed SIP packet`

Symptom 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.

Workaround 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

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

CSCsb93407 H323 port tcp 1720 still listening after call service stop

Symptom With H323 call service stopped, the router still listens on tcp port 1720 and completes connection attempts.

Conditions After H323 is disabled using the configuration commands:

- voice service voip
- h323
- call service stop

Workaround Access can be blocked by deploying an interface access list that blocks access to TCP port 1720 for traffic that is destined for any of the IP addresses of the router.

For information about deploying access lists, see the "Transit Access Control Lists: Filtering at Your Edge" document: http://www.cisco.com/warp/public/707/tacl.html

For further information about deploying access lists, see the "Protecting Your Core: Infrastructure Protection Access Control Lists" document: http://www.cisco.com/warp/public/707/iacl.html For information about using control plane policing to block access to TCP port 1720, see the "Deploying Control Plane Policing White Paper:" http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

CSCse68138 Issue in handling specific packets in VOIP RTP Lib

Symptom 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.

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

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

`CSCsg70474 IOS FW with h323 inspect crashes when malformed H.323 packets received`

Symptom 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.

Workaround 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

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

Symptom System reloads unexpectedly or other serious side-affects 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
                        00000000011111111112222222333^
                        12345678901234567890123456789012|
                                                         |
                                                PROBLEM (Variable Overflowed).
```

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

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.

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

Condition:
    conf t
      gatekeeper
        gw-type-prefix
               1234.................................................

        and enter command sh run
```

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

CSCsj55415 PISA: DATACORRUPTION-SP-STDBY-1-DATAINCONSISTENCY: copy error

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 data corruption tracebacks occurs.

Workaround There is no workaround.

CSCef77013 tighter parameter checking for ipv6

Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted

Symptom IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected IOS and IOS XR devices, and may also result in a crash of the affected IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

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

Workaround There are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml

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 behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

Conditions This issue occurs in IOS images that has the fix for CSCse85200.

Workaround Disable CDP on interfaces where CDP is not required. Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

CSCsd58381 ipv6 routing header limitation

Symptom Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

Workaround There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used. This advisory is posted at :
http://www.cisco.com/en/US/products/products_security_advisory09186a00807cb0fd.shtml

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

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, there is no workaround. 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.

CSCsc64976 HTTP server should scrub embedded HTML tags from cmd output

Symptom A vulnerability exists in the IOS HTTP server in which HTML code is 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.

Symptom 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

CSCsh04686 Malformed TCP packet forces reload with x25 routing (XOT)

Symptom With X25 over TCP (XOT) enabled on a router or catalyst switch, malformed traffic sent to TCP port 1998 will cause the device to reload. This was first observed in IOS 12.2(31)SB2.

Conditions Must have "x25 routing" enabled on the device.

Workaround Use IPSEC or other tunneling mechanisms to protect XOT traffic. Also, apply ACLs on affected devices so that traffic is only accepted from trusted tunnel endpoints.

CSCsb11124 SGBP Crafted Packet Denial of Service

Symptom 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.

Workaround 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

CSCsg16908 IOS FTP Server Deprecation

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

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

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.

CSCsj81502 show pagp clis are not displaying the correct information

Symptom In release 12.2(33)SXH or 12.2(18)SXF10 releases, the output of 'show pagp neighbor' command may truncate the neighbor device name and port name fields by 1 character. This is just a display issue and has no functional impact on the PAGP protocol.

Conditions This issue is only seen with 12.2(33)SXH and 12.2(18)SXF10 images. This issue only affect PAGP etherchannel member ports.

Workaround There is no workaround at this time. If a user wants to find out the partner's correct information, he/she could use the output of "show cdp neighbor" command.

CSCsi60004 H323 Proxy Unregistration from Gatekeeper

Symptom 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.

Workaround 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

CSCeb56909 Crafted packet causes reload on Cisco routers

Symptom 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

CSCsj86725 Running lpd with certain configurations could cause overflow

CSCsj66692 Data integrity traceback seen in voip/ccapi/ccapi_call.c

Symptom Data corruption copy error tracebacks are seen on the console or output from the show logging command:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error,  -PC= 0x41224EFC,  -
Traceback= 0x4153A7D0 0x4155BA0C 0x4157FAF0 0x41224EFC 0x41DDC0A8 0x41DDC198
0x41DC6D84 0x41DF3B0C 0x41DC506C 0x41DCE5A4 0x41D91AF8 0x41D90F88 0x41D9BEFC
0x41D9C0C0 0x41DAEA68
```

Workaround There is no workaround.

CSCsk57644: When SOHO71 is loaded with 122-13.ZH9, router hangs and never responds

CSCsh74975: udp packets to port 2517 cause memory depletion or reload on router

Symptom A router may reload or a leak memory may occur when UDP malformed packets are sent to port 2517.

Conditions This symptom is observed on a Cisco router that functions as a VoIP dial peer and that is configured for H.323.

Workaround There is no workaround.

CSCsi67763 IPS evasion using Unicode encoding for HTTP-based attack

Resolved Caveats - Release 12.2(13)ZH9

CSCsd95616

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-multicast.shtml.

CSCsf04754

Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The

SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

`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

`CSCsj81502 show pagp clis are not displaying the correct information`

Symptom In release 12.2(33)SXH or 12.2(18)SXF10 releases, the output of 'show pagp neighbor' command may truncate the neighbor device name and port name fields by 1 character. This is just a display issue and has no functional impact on the PAGP protocol.

Conditions 1) This issue is only seen with 12.2(33)SXH and 12.2(18)SXF10 images. 2) This issue only affect PAGP etherchannel member ports.

Workaround There is no known workaround at this time. If a user wants to find out the partner's correct information, he/she could use the output of **show cdp neighbor** command.

`CSCsd58381 ipv6 routing header limitation`

Symptom Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

Workaround There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

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.

Conditions This issue occurs in IOS images that has the fix for "CSCse85200.

Workaround Disable CDP on interfaces where CDP is not required. **Further Problem Description:** Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

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 workaound.

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

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

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

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                         00000000011111111111222222222333^
                         12345678901234567890123456789012|
                                                          |
                                                   PROBLEM
                                                 (Variable Overflowed).
```

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

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

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.

CSCse68138 Issue in handling specific packets in VOIP RTP Lib

Symptom 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.

Workaround 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.

CSCef61610 Incorrect handling of ICMPv6 messages can cause TCP performance problems

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

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

1. Attacks that use ICMP "hard" error messages

2. Attacks that use ICMP “fragmentation needed and Don't Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

3. Attacks that use ICMP “source quench” messages

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

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

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

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

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

http://www.cisco.com/en/US/products/products_security_advisory09186a00807b8e55.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

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.

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.

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.

CSCsb11124 SGBP Crafted Packet Denial of Service

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

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

Cisco has published a Security Advisory on this issue; it is available at http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml

CSCef48336 Corrupted OSPF Hello packets caused software forced crash

OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89.

A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

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

Using OSPF Authentication can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice.

A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack.

Workaround Using OSPF Authentication

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

Refer to
http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.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

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

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

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.

CSCsg16908 IOS FTP Server Deprecation

Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information. The IOS FTP Server is an optional service that is disabled by default.

Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities. This vulnerability does not apply to the IOS FTP Client feature.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

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.

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

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

Only devices running certain versions of Cisco IOS are affected. Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

This advisory will be posted at
http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

CSCee45312 Radius authentication bypass when configured with a none fallback method

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

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

Only the systems that are running certain versions of Cisco IOS are affected.

Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

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

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

CSCsg70474 IOS FW with h323 inspect crashes when malformed H.323 packets received

Symptom 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.

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

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

CSCef77013 tighter parameter checking for ipv6

Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected IOS and IOS XR devices, and may also result in a crash of the affected IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

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

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml

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.

CSCei61732 Additional data integrity check in system timer

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

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

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

CSCef68324 ICMPv6 pkt traceback

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

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

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

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

CSCsi60004 H323 Proxy Unregistration from Gatekeeper

Symptom 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.

Workaround 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.

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.

Conditions This issue occurs in IOS images that has the fix for CSCse85200.

Workaround Disable CDP on interfaces where CDP is not required.

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

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.

CSCsb79076MGCP 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 No workaround currently available.

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

Symptom 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.

Workaround 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.

CSCsc06695 IKEv1 SA leaks under certain conditions

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

Workaround Clear isakmp as manually.

CSCsb33172 short-circuit crypto engine operations when faking AM2

A vulnerability exists in the way some Cisco products handle IKE phase I messages which allows an attacker to discover which group names are configured and valid on the device.

A Cisco Security Notice has been published on this issue and can be found at the following URL:

http://www.cisco.com/warp/public/707/cisco-son-20050624-van-grpname.shtml

CSCed95187 IP ID field is predictable for connections RST packets

Symptom RST packets may contain a non-randomized identification value on the IP header.

Conditions This symptom is observed on a Cisco platform that receives a TCP SYN packet on a non-listening port.

Workaround There is no workaround.

Further Problem Description From RFC791, the description of the Identification field is as follows: Identification The choice of the Identifier for a datagram is based on the need to provide a way to uniquely identify the fragments of a particular datagram. The protocol module assembling fragments judges fragments to belong to the same datagram if they have the same source, destination, protocol, and Identifier. Thus, the sender must choose the Identifier to be unique for this source, destination pair and protocol for the time the datagram (or any fragment of it) could be alive in the internet.

It seems then that a sending protocol module needs to keep a table of Identifiers, one entry for each destination it has communicated with in the last maximum packet lifetime for the internet.

Also from RFC791, section 3.1. (Internet Header Format): The IP ID is before the flags and fragment offset fields.

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

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

Conditions The Cisco IOS configuration command:

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

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

clock summer-time *PDT*
recurring *2 Sun Mar 2:00 1 Sun Nov. 2:00*

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

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

CSCeb21064 Crash while processing malformed SIP packet

Symptom 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.

Workaround 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`

Symptom 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.

Workaround There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

`CSCse68138 Issue in handling specific packets in VOIP RTP Lib`

Symptom 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.

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

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

CSCeg62070 Tracebacks noticed with Radius configs through HTTP Post

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

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

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

CSCsb12598 Router forced crash on receiving fragmented TLS ClientHello

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

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

Cisco IOS is affected by the following vulnerabilities:

* Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

* Processing ChangeCipherSpec messages, documented as Cisco bug IDCSCsb40304

* 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.

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

CSCse85200 Inadequate validation of TLVs in cdp

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

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

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

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 IDCSCsb40304

* Processing Finished messages, documented as Cisco bug ID CSCsd92405

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

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

Note: Another related advisory has been posted with this advisory.

This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS.

This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

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

This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

CSCsd92405 router crashed by repeated SSL connection with malformed finished messag

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

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

Cisco IOS is affected by the following vulnerabilities:

* Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

* Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

* Processing Finished messages, documented as Cisco bug ID CSCsd92405

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

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

Note: Another related advisory has been posted with this advisory.

This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS.

This related advisory is available at the following link:
http://www.cisco.com/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.

CSCse04560 tftp-server allows for information disclosure

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

Symptom

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

tftp-server flash:*filename1 access-list-number*

access-list *access-list-number* **permit** *192.168.1.0 0.0.0.255*

```
access-list access-list-number deny any
```

Workaround The following workarounds can be applied:

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

```
access-list access-list-number remark --- the following hosts and networks area ALLOWED
for TFTP access
access-list access-list-number permit udp host source_1 host interface_address_1 eq 69
access-list access-list-number permit udp host source_2 host interface_address_2 eq 69
access-list access-list-number permit udp source source-wildcard host interface_address_1
eq 69
access-list access-list-number permit udp source source-wildcard host interface_address_2
eq 69
access-list access-list-number remark --- everyone else is DENIED for TFTP access
access-list access-list-number deny udp any host interface_address_1 eq 69
access-list access-list-number deny udp any host interface_address_2 eq 69
access-list access-list-number remark --- any other traffic to/through the router is
allowed
access-list access-list-number permit ip any any

interface Ethernet0/0
  ip access-group access-list-number in
```

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

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

```
access-list access-list-number remark --- Do not police TFTP traffic from trusted hosts
and networks
access-list access-list-number deny udp host source_1 any eq 69
access-list access-list-number deny udp source source-wildcard any eq 69
access-list access-list-number remark --- Police TFTP traffic from untrusted hosts and
networks
access-list access-list-number permit udp any any eq 69
access-list access-list-number remark --- Do not police any other traffic going to the
router
access-list access-list-number deny ip any any
class-map match-all tftp-class
  match access-group access-list-number

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

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

Note CoPP is only available on certain platforms and Cisco IOS releases. Additional information on the configuration and use of the CoPP feature can be found at the following URL: http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

3. Infrastructure ACLs (iACL) Although often difficult to block traffic transitting your network, identifying traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network is possible. Infrastructure ACLs are considered a network security

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

4. Configuring Receive Access Lists (rACLs) For distributed platforms, rACLs may be an option starting in Cisco IOS Release 12.0(21)S2 for the Cisco 12000 series GSR and Cisco IOS Release 12.0 (24)S for the Cisco 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets: http://www.cisco.com/warp/public/707/racl.html

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

CSCsd85587 7200 Router crashes with ISAKMP Codenomicon test suite

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

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

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

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

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

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

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

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

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

CSCsd40334 IPv6 packet can cause crash

Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

This advisory is posted at
http://www.cisco.com/en/US/products/products_security_advisory09186a0080a96c25.shtml

CSCee41508 RSVP red zone crash

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

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

Workaround If RSVP is required, no workaround exists.

If RSVP is not required, disabling RSVP on all interfaces removes any exposure to this issue.

RSVP can be disabled using the **no ip rsvp bandwidth** interface configuration command. The **show ip rsvp** EXEC command can be used on an IOS device to determine if RSVP functionality has been enabled. The **show ip rsvp interface** EXEC command may be used to identify the specific interfaces on which RSVP has been enabled.

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

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

Conditions This problem happens only with command accounting enabled.

Workaround Disable command accounting.

`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.

`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.

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

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/tacl.html.

For information about using control plane policing to block access to TCP port1720, see the "Deploying Control Plane Policing White Paper" at http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html.

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

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.

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.

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.

CSCsa59616 auth-proxy not working with next token

Symptom Proxy-auth with http does not work when token is not in sync, when it is in next token mode. The user gets the first login web page, and when he enter the userid or pin, and then he get a popup page that says: “First Retry successful” After that a blank page is displayed. The router is not sending a next token page to sync token. Show ip auth-proxy cache” show the current user is in a HTTP_WAIT_NEXT_PASSWORD state. After several users are in this state, it is reported that the router will no longer accept any new users connections even if they're tokens are not out of sync.Clearing the ip auth-proxy cache will allow new users who are not out of sync to log in.

Workaround use telnet method for proxy-authentication instead of http.

Resolved Caveats - Release 12.3(13)ZH8

Cisco IOS Release 12.2(13)ZH is a rebuild release for Cisco IOS Cisco IOS Release 12.2(13)ZH. This section describes unexpected behavior that is fixed in Release 12.2(13)ZH7.

- 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.

- CSCec25430

  Symptoms: A Cisco device reloads on receipt of a corrupt CDP packet.

  Conditions: This symptom is observed when an empty "version" field exists in the output of the **show cdp entry** command for at least one entry.

  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.

- CSCeb52066

  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, the attack vector does not directly compromise data integrity or confidentiality.

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

  This advisory is available at the following URL: 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.

  A companion 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.

- CSCeh47763

  Symptoms: A Cisco 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.

- CSCee45312

  Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method 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

  Symptoms: 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.

  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 the following URL: http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml.

- CSCeg15044

  Symptoms: Although there are free tty lines, you cannot make a Telnet connection and a "No Free TTYs error" message is generated.

  Conditions: This symptom is observed when there are simultaneous Telnet requests.

  Workaround: The command "clear tcp tcb" should clear the line.

- 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 the following URL: http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

- CSCin67568

  Symptoms: A Cisco device experiences a memory leak in the CDP process.

  Conditions: 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**.

- CSCea28131

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. 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. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at the following URL:

  http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCeb85136

  Symptoms: An IP packet that is sent with an invalid IP checksum may not be dropped.

Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value. For example, in the situation where the IP checksum must be 0x1134 with a TTL of 3, if the packet is sent with an IP checksum of 0x1234 that is calculated by using a TTL value of 2, the packet is not dropped. In all other cases, packets with incorrect checksums are dropped.

Workaround: There is no workaround.

- CSCec16481

  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.

- CSCec76694

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  The advisory can be found at the following URL:
  http://www.cisco.com/en/US/products/products_security_advisory09186a00801ea156.shtml.

- CSCed82706

  Tracebacks will be seen with nhrp + ipsec profile + NAT + EIGRP setup when trying to bring up ike/ipsec sas.

  Workaround: There is no workaround.

- CSCee76562

  Symptoms: Spurious memory accesses may occur and tracebacks may be generated.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(9.3)T when the interface command 'no ip next-hop-self eigrp' is used. The defect is a regression of CSCdk23784.

  Workaround: There is no workaround.

- CSCef48336

  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.

Workarounds: 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/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtml for more information about OSPF authentication.

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

- CSCdz84583

  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, the attack vector does not directly compromise data integrity or confidentiality.

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

  This advisory is available at the following URL: 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 IOSÆ software.

  A companion 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.

- CSCeb06536

  Symptoms: IP Security (IPSec) authentication header (AH)/Encapsulating Security Payload (ESP) encapsulated packets that fail authentication or replay check are not being discarded even though they are flagged by error messages. The authentication and replay failure conditions are indicated by the ?Output Authentication error? or ?Output Replay Error? error messages displayed on the router.

  These packets may be inadvertently be forwarded to routers that use the virtual private network (VPN) encryption hardware advanced integration modules (AIM-VPN/EPII & AIM-VPN/HPII).

  Conditions: This symptom is observed on routers that use the AIM-VPN/EPII & AIM-VPN/HPII advanced integration modules.

  Workaround: Disable hardware crypto by entering the no crypto engine accelerator global configuration command and use software crypto instead.

- CSCeb16876

  Symptoms: A Cisco router may generate a "SYS-2-GETBUF" message during the "Tag Input" process and may subsequently reload unexpectedly.

  Conditions: This symptom is observed when the router fragments a Multiprotocol Label Switching (MPLS) packet.

  Workaround: There is no workaround.

- CSCeb40662

  backout MAX_SPIN=2 fix from E0 Rx int routine

- CSCeb88239

  Symptoms: A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.

  Conditions: 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: There is no workaround.

- CSCed03333

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

  Workaround: None. Lowering the inspect FTP timeout will reduce exposure. Disabling CEF will reduce exposure.

  Fix: Bump certain out-of-order packets to process path for catch-up and then dropping packets if unsuccessful.

- CSCed35253

  Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

  Conditions: 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.

- CSCed93836

  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 the following URL: 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 IOSÆ software.

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

- CSCee08584

  Cisco Internetwork Operating System (IOSÆ) 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.

- CSCee47441

  Symptoms: When the Cisco IOS Firewall CBAC is configured, the router seems to have a software-forced reload caused by one of the inspections processed.

  Conditions: This symptom is observed when the router is part of a DMVPN hub-spoke with a Cisco VoIP phone solution deployed on it and the router is connected to the central office over the Internet. The Cisco VoIP phone runs the SKINNY protocol.

  Workaround: There is no workaround.

- CSCef61610

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

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

  1. Attacks that use ICMP "hard" error messages.

  2. Attacks that use ICMP "fragmentation needed and Don’t Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.

  3. Attacks that use ICMP "source quench" messages

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

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

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 the following URL:
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 the following URL:
http://www.cisco.com/en/US/products/products_security_advisory09186a00807b8e55.shtml.

- CSCeg47738

  Incorrect count loaded into Timer3 that handles ISDN layer1.

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

- CSCea51540

  Symptoms: The IP Control Protocol (IPCP) times out in a Link Control Protocol (LCP) negotiation.

  Conditions: The problem happens when "virtual-profile virtual-template" is configured without "virtual-profile if-needed" and an ASYNC call creates a Virtual-Access interface.

  Workaround: Configure "virtual-profile if-needed" and use the ASYNC interface without a Vaccess.

- CSCsa52807

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

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

  1. Attacks that use ICMP "hard" error messages.

  2. Attacks that use ICMP "fragmentation needed and Don’t Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.

  3. Attacks that use ICMP "source quench" messages

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

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

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 the following URL:
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 the following URL:
https://www.kb.cert.org/vuls/id/104280.

Resolved Caveats - Cisco IOS Release 12.2(13)ZH7

Cisco IOS Release 12.2(13)ZH7 is a rebuild release for Cisco IOS Cisco IOS Release 12.2(13)ZH. This section describes unexpected behavior that is fixed in Release 12.2(13)ZH7.

- CSCef68324

  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 the following URL:
  http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

Resolved Caveats - Cisco IOS Release 12.2(13)ZH6

Cisco IOS Release 12.2(13)ZH6 is a rebuild release for Cisco IOS Cisco IOS Release 12.2(13)ZH. This section describes unexpected behavior that is fixed in Release 12.2(13)ZH6.

- CSCee67450—BGP error message 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.

- 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: https://www.kb.cert.org/vuls/id/104280.

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

  See note for CSCed78149 above.

- CSCef60659—More stringent checks required for ICMP unreachables.

  See note for CSCed78149 above.

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

  See note for CSCed78149 above.

- CSCsa59600—IPSec PMTUD not working [after CSCef44225].

  See note for CSCed78149 above.

- 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

Resolved Caveats - Cisco IOS Release 12.2(13)ZH4

Cisco IOS Release 12.2(13)ZH4 is a rebuild release for Cisco IOS Cisco IOS Release 12.2(13)ZH. This section describes unexpected behavior that is fixed in Release 12.2(13)ZH4.

- CSCed34050—The Cisco 837 router: Middle buffers and HIFN79xx buffer issues.

  A Cisco 837 router may encounter memory allocation failures in I/O memory.

- CSCec77078—Packet delay over IPSec tunnel when hardware crypto is used.

  A Cisco 836 router with a generic routing encapsulation (GRE) tunnel over an IPSec tunnel can introduce delays on packets sent over the GRE tunnel.

  Workaround: Disable hardware encryption using the **no crypto engine accelerator** command.

Resolved Caveats - Cisco IOS Release 12.2(13)ZH3

Cisco IOS Release 12.2(13)ZH3 is a rebuild release for Cisco IOS Cisco IOS Release 12.2(13)ZH. This section describes unexpected behavior that is fixed in Release 12.2(13)ZH3.

- CSCdz70054—SAA/Rtr HTTP get operation fails without DNS with error code 16.

  In Cisco IOS Release 12.2 T, the Round Trip Recorder (RTR)/Service Assurance Agent (SAA) HTTP get operation with IP address in the URL, like
  type http operation get url *http://10.10.10.10/* fails with internal error (error code=16) if Domain Name System (DNS) is not configured on the router.

  Workaround: Configure name resolution on the router, using **ip name-server** command or use Cisco IOS Release 12.2 mainline release image.

Resolved Caveats - Cisco IOS Release 12.2(13)ZH2

Cisco IOS Release 12.2(13)ZH2 is a rebuild release for Cisco IOS Cisco IOS Release 12.2(13)ZH. This section describes unexpected behavior that is fixed in Release 12.2(13)ZH2.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at the following URL:

http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at the following URL:

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

Resolved Caveats - Cisco IOS Release 12.2(13)ZH1

Cisco IOS Release 12.2(13)ZH1 is a rebuild release for Cisco IOS Release 12.2(13)ZH. This section describes unexpected behavior that is fixed in Release 12.2(13)ZH1.

- CSCea31287

  The router's wildcard or subnet crypto Internet Security Association and Key Management Protocol (ISAKMP) preshared key can overwritten by host key.

  Workaround: Configure the wildcard and subnet preshared keys after host keys.

- CSCea65792

  Input queue of WAN interface (E1) of Cisco 831 router may get filled and wedge the interface. After input wedge, the router will not receive any traffic on the WAN link until router is rebooted.

  Workaround: There is no workaround.

Open Caveats - Cisco IOS Release 12.2(13)ZH1

The following sections list the open caveats for the Cisco IOS release 12.2(13)ZH1.

- CSCeb04895

  When **key config-key** command is used to encrypt password, EZVPN will not come up.

  Workaround: Do not configure **key config-key password-encrypt** <*private-key*> and **password encryption aes** commands in global configuration mode.

Open Caveats - Cisco IOS Release 12.2(13)ZH

The following sections list the open caveats for the Cisco IOS release 12.2(13)ZH.

- CSCdx65416

  SIP support for CBAC does not handle PRACK messages properly, and the router will not be able to distinguish between "200 OK in response to PRACK" versus "200 OK in response to INVITE".

Workaround: Disable PRACK by configuring following on the SIP gateway:

a. **voice service voip** command
b. **sip** command
c. **rel1xx disable** command

- CSCea42210

  Traceback is observed when WebSense server is configured with a wrong IP.

  When the WebSense server is down, traceback message occurs for each connection attempt made to the WebSense server. No router functionality is affected by these traceback messages.

- CSCin38587

  The router hangs when **ip unnumbered** command is configured on the tunnel interface.

  When IP unnumbered is configured on the tunnel interface with HW crypto engine enabled, the router will go in infinite loop sending IP packets. This will happen only when both peer and local router's Tunnel interface IP address are changed to unnumbered and Enhanced Interior Gateway Routing Protocol (EIGRP) enabled on the router.

  Workaround:Disable hardware crypto or change routing protocol to Routing Information Protocol (RIP).

- CSCea29573

  Error messages related hardware crypto engine are printed sporadically.

  Error messages related hardware crypto engine are printed on the router console every few days. This will occur when generic routing encapsulation (GRE) tunneling is used with hardware crypto engine and when fast switching configured.

  Workaround: Disable fast switching or use Cisco Express Forwarding (CEF) switching.

- CSCea33138

  Packets dropped while building multipoint GRE (mGRE) spoke-spoke link and CEF switch.

  Spoke-to-spoke data packets may be dropped in a Dynamic Multipoint Virtual Private Network (DMVPN) is observed while Next Hop Resolution Protocol (NHRP) and IP Security (IPSec) are resolving the remote spoke addresses and building the IPSec security associations (SAs). This process may take from 3 to 8 sec to complete.

  Workaround: Use process switching on the spoke routers.

- CSCea64819

  Crypto/NHRP is not able to handle the peer address change.

  When the ISP address on the peer spoke router is changed, the other spoke will not be able to send traffic to it. The old crypto socket would still bind with the spoke router’s old ISP address.

  Workaround: None.

- CSCea34836

  NHRP sends resolution request to last configured Next Hop Server (NHS).

  When process switching is enabled, the router will send the NHRP resolution request to the wrong hub.

  Workaround: Configure the primary hub to appear as last item in the list of NHS in the router configuration.

- CSCea58967

  MIB values differ with **show policy-map interface** command.

- CSCea71039

  Extra value is expected as input while unconfiguring police feature.

- CSCes72884

  MIB does not support multiple actions while police feature is configured.

Additional References

The following sections describe the documentation available for the Cisco SOHO 71, SOHO 76, SOHO 77, and the Cisco 826, Cisco 827, and Cisco 828 routers. 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 59
- Platform-Specific Documents, page 59

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Cisco IOS Release 12.2(13)ZH. They are located on Cisco.com:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2T*
- *Field Notices:* http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2T*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco SOHO 71, SOHO 76, SOHO 77, and the Cisco 826, Cisco 827, and Cisco 828 routers are available on 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 12.2 and Cisco IOS Release 12.2(13)ZH, 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, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Use this document in conjunction with the documents listed in the "Additional References" section.