Release Notes for Cisco 800 and SOHO 90 Series Routers for Cisco IOS Release 12.3(8)YA

August 3, 2007
Cisco IOS Release 12.2(4)YA12
OL-14334-02

These release notes describe new features and significant software components for the Cisco 800 and SOHO 90 Series Routers that support the Cisco IOS Release 12.2(4)YA releases. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, changes to the microcode or modem code, and any other important changes. Use these release notes with Cross-Platform Release Notes for Cisco IOS Release 12.2T located on Cisco.com.

For a list of the software caveats that apply to Cisco IOS Release 12.2(4)YA12, see Caveats, page 8 and see the online Caveats for Cisco IOS Release 12.2T. The caveats document is updated for every 12.2T maintenance release and is located on Cisco.com.

Contents

System Requirements

This section describes the system requirements for Cisco IOS Cisco IOS Release 12.2(4)YA and includes the following sections:

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

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(4)YA on the Cisco 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers.

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

				Flash Memory		DRAM	
Platform	**Image Name**	**Feature Set**	**Image**	**Mini-mum**	**Recom-mended[1]**	**Mini-mum**	**Recom-mended**
Cisco 831	Cisco 831 Series IOS IP/FW2 IPSec 3DES	IP/FW2/IPSec 3DES	c831-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 831 Series IOS IP/FW2 Plus IPSec 3DES	IP Plus/FW2/IPSec 3DES	c831-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
Cisco 836	Cisco 836 Series IOS IP/FW2 IPSec 3DES	IP/FW2/IPSec 3DES	c836-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 836 Series IOS IP/FW2 Plus IPSec 3DES	IP Plus/FW2/IPSec 3DES	c836-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 836 Series IOS IP/FW2/Dial Backup Plus IPSec 3DES	IP Plus/FW2/Dial Backup IPSec 3DES	c836-k9o3s8y6-mz	12 MB	12 MB	48 MB	48 MB
Cisco 837	Cisco 837 Series IOS IP/FW2 IPSec 3DES	IP/FW2/IPSec 3DES	c837-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 837 Series IOS IP/FW2 Plus IPSec 3DES	IP Plus/FW2/IPSec 3DES	c837-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
Cisco SOHO 91	Cisco SOHO 91 Series IOS IP/FW/3DES	IP/FW 3DES	soho91-k9oy6-mz	8 MB	8 MB	32 MB	32 MB
Cisco SOHO 96	Cisco SOHO 96 Series IOS IP/FW/3DES	IP/FW 3DES	soho96-k9oy1-mz	8 MB	8 MB	32 MB	32 MB
Cisco SOHO 97	Cisco SOHO 97 Series IOS IP/FW 3DES	IP/FW 3DES	soho97-k9oy1-mz	8 MB	8 MB	32 MB	32 MB

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

Hardware Supported

Cisco IOS Cisco IOS Release 12.2(4)YA supports the following routers:

- Cisco 831 router
- Cisco 836 router
- Cisco 837 router
- Cisco SOHO 91 router
- Cisco SOHO 96 router
- Cisco SOHO 97 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 the Cisco 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers, which are available on Cisco.com at the following location:

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

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

Technical Documentation: **Routers**: **Fixed Config. Access Routers**: **<platform_name>**

Determining the Software Version

To determine which version of the Cisco IOS software is currently running on your Cisco 831, 836, 837, SOHO 91, SOHO 96, or SOHO 97 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(4)YA, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1) Synched to technology version 12.3(9.6)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see the *Software Installation and Upgrade Procedures* located at http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Hardware&f=742.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.3(8)YA1 includes the same feature sets supported by the Cisco 800 and SOHO 90 series routers as Releases 12.3, 12.3(8)T, and 12.3(8)YA. There are no new features in Release 12.3(8)YA1

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

Table 2 through Table 7 list the features and feature sets that are supported in Cisco IOS Cisco IOS Release 12.2(4)YA.

The tables use the following conventions:

- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, "12.2(4)YA" indicates that the feature was introduced in Release 12.2(4)YA. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.

Note These feature set tables contain only a list of selected features, which are cumulative for Release 12.3(8)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all the features in each image; additional features are listed in *Cross-Platform Release Notes for Cisco IOS Release 12.3(8)T* and in Release 12.3(8)T Cisco IOS documentation.

Table 2 Feature Set Table for the Cisco 831 Router

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
Dynamic DNS Support for Cisco IOS	12.2(4)YA	Yes	Yes
No Service Password Recovery	12.2(4)YA	Yes	Yes
Bridge MIB	12.2(4)YA	Yes	Yes

Table 3 Feature Set Table for the Cisco 836 Router

Feature	In	Feature Set		
		IP/FW2 3DES	IP/FW2 Plus 3DES	IP Plus/FW2/Dial Backup IPSec 3DES
Dynamic DNS Support for Cisco IOS	12.2(4)YA	Yes	Yes	Yes
No Service Password Recovery	12.2(4)YA	Yes	Yes	Yes
Bridge MIB	12.2(4)YA	Yes	Yes	Yes

Table 4 Feature Set Table for the Cisco 837 Router

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
Dynamic DNS Support for Cisco IOS	12.2(4)YA	Yes	Yes
No Service Password Recovery	12.2(4)YA	Yes	Yes
Bridge MIB	12.2(4)YA	Yes	Yes

Table 5 Feature Set Table for the Cisco SOHO91 Router

Feature	In	Feature Set
		IP/FW 3DES
Dynamic DNS Support for Cisco IOS	12.2(4)YA	Yes
No Service Password Recovery	12.2(4)YA	Yes
Bridge MIB	12.2(4)YA	No

Table 6 Feature Set Table for the Cisco SOHO 96 Router

Feature	In	Feature Set
		IP/FW 3DES
Dynamic DNS Support for Cisco IOS	12.2(4)YA	Yes
No Service Password Recovery	12.2(4)YA	Yes
Bridge MIB	12.2(4)YA	No

Table 7 Feature Set Table for the Cisco SOHO 97 Router

Feature	In	Feature Set
		IP/FW 3DES
Dynamic DNS Support for Cisco IOS	12.2(4)YA	Yes
No Service Password Recovery	12.2(4)YA	Yes
Bridge MIB	12.2(4)YA	No

New and Changed Information

The following sections list the new software features supported by the Cisco 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers for Cisco IOS Release 12.2(4)YA.

New Software Features in Cisco IOS Release 12.2(4)YA1

There are no new software features in Cisco IOS Release 12.2(4)YA1.

New Software Features in Release 12.2(4)YA

The following sections describe the new software features supported by the Cisco 800 and SOHO 90 series routers for Release 12.2(4)YA.

Dynamic DNS Support for Cisco IOS

The Dynamic DNS Support for Cisco IOS feature enables Cisco IOS devices to perform Dynamic Domain Name System (DDNS) updates to ensure that an IP host DNS name is correctly associated with its IP address.

It provides two mechanisms to generate or perform DDNS: the IETF standard as defined by RFC 2136, and a generic HTTP using various DNS services. With this feature, you can define a list of host names and IP addresses that will receive updates, specify an update method, and specify a configuration for DHCP triggered updates.

With the Dynamic DNS Support feature, you can define a list of hostnames and/or IP addresses that will receive updates, can specify an update method, and can specify a configuration for DHCP-triggered updates.

For more details about the Dynamic DNS Support for Cisco IOS feature, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123ya8/gt_ddns.htm

No Service Password Recovery

The No Service Password-Recovery feature is a security enhancement that prevents anyone with access to a console from accessing the router configuration and clearing the password. It also prevents anyone from changing the configuration register values and accessing non-volatile RAM (NVRAM).

The No Service Password Recovery feature is enabled using the **no service password-recovery** hidden command. When this hidden command is used, a warning and a confirmation prompt appear on your router.

To disable the feature, use the **service password-recovery** command.

The No Service Password Recovery feature also recovers the forgotten passwords. When this feature is enabled, the router accepts the break signal within 5 seconds, just after the Cisco IOS software is decompressed during booting. The user is then prompted to confirm the action. After confirmation, the startup configuration is erased, the password recovery procedure is enabled, and the router boots with the factory default configuration. When the user enters “no”, the router boots normally and with the No Service Password Recovery feature enabled.

For more details about the No Service Password Recovery feature, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123ya8/ftnsvpwd.htm

The No Service Password Recovery feature requires use of ROMMON version 12.2(11r)YV1. The procedure for upgrading the ROMMON image from ROMMON mode is given at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/827/820rmup.htm#54965

Bridge MIB

The Bridge MIB feature, extracted from RFC 1493, defines objects for managing MAC bridges between LAN segments. The Bridge MIB feature provides information regarding various ports of the bridge, Spanning Tree Protocol (STP), and transparent bridging, and supports dot1dBase, dot1dStp, and dot1dTp standards.

New Software Features in Release 12.3(8)T

For information regarding the features supported in the Cisco IOS Release 12.3(8)T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com:

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

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

Service & Support: **Technical Documents**: **Cisco IOS Software**: **Release 12.3**: **Release Notes**: **Cross-Platform Release Notes (Cisco IOS Release 12.3(8)T)**

Limitations and Restrictions

The following sections describe limitations concerning the new hardware and software features supported by the Cisco 800 series routers for Cisco IOS Release 12.2(4)YA and 12.3(8)YA.

No Service Password Recovery

The following limitations apply for the No Service Password Recovery feature:

- After the feature is configured, it remains configured even after router reload (the command will be listed in running configuration). It is not necessary to write this configuration into NVRAM to keep the feature enabled between reloads.
- To enable the feature, disable the break bit and the bit to ignore the startup configuration. Set the boot bits value in the configuration register.
- If you want to change configuration register value after the No Service Password Recovery feature is enabled, the above restrictions still apply.

  Table 8 lists the meanings of the software configuration memory bits.

Table 8 Software Configuration Memory Bits

Bit Number	Hexadecimal	Meaning
00 to 03	0x0000 to 0x000F	Boot field
06	0x0040	Causes system software to ignore NVRAM contents
07	0x0080	OEM bit enabled
08	0x0100	Break disabled
09	0x0200	Use secondary bootstrap

Table 8 Software Configuration Memory Bits (continued)

Bit Number	Hexadecimal	Meaning
10	0x0400	IP broadcast with all zeros
11 to 12	0x0800 to 0x1000	Console line speed (default is 9600 baud)
13	0x2000	Boot default Flash software if network boot fails
14	0x4000	IP broadcasts do not have network numbers
15	0x8000	Enable diagnostic messages and ignore NVRAM contents

- When the feature is enabled, do not reload or powercycle the router without a valid image in the boot device. The router will not go into the ROMMON mode because of the No Service Password Recovery feature and since there is no IOS to boot with, the ROMMON continuously reloads. The only workaround to recover from this setup is to request a Cisco Systems return materials authorization (RMA).
- Before you downgrade the image in the router, disable the feature. It will not be possible to reset the feature with a downgraded image.
- Reload the router so that any changes to the configuration register value will take effect.

Caveats

Caveats describe unexpected behavior or defects in the Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

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 - Cisco IOS Release 12.2(4)YA12

`CSCei61732 Additional data integrity check in system timer`

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

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

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

CSCef68324 ICMPv6 pkt traceback

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

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

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

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

CSCsd92405 router crashed by repeated SSL connection with malformed finished message

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

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.

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

CSCsb33172 short-circuit crypto engine operations when faking AM2

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

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

http://www.cisco.com/warp/public/707/cisco-sn-20050624-vpn-grpname.shtml

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

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

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.

CSCse05736 ssh leaks memory and buffers

Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload.

Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

CSCsc64976 HTTP server should scrub embedded HTML tags from cmd output

A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected. Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051201-http.shtml

SCek37177 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

CSCsb12598 Router forced crash on receiving fragmented TLS ClientHello

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

CSCsb40304 Router crash on sending repetitive SSL ChangeCipherSpec

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

CSCsb12598 Router forced crash on receiving fragmented TLS ClientHello

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

Symptom Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router. Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

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

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

CSCse85200 Inadequate validation of TLVs in cdp

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

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

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

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.

Resolved Caveats - Cisco IOS Release 12.2(4)YA

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)YA1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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.

- CSCef83876

  DHCP Client could not renew the IP address using the ATM unnumbered interface, after changing the configuration on the bridge.

- CSCef95695

When configuring ezvpn using nat-t on a Cisco 831 router, the IPSec SA's are created but only encaps packets are shown in the byte counts. The esp frames are sent with protocol 50 instead of 4500 for nat-t.

- CSCeg44078 c836

  DMZ - Huge delay transmitting traffic on Eth0 and Eth2.

- CSCeg47738

  Incorrect count loaded into Timer3 that handles ISDN layer1.

- CSCef46191

  Unable to telnet.

- CSCef12235

  ISDN TEI negotiation fails when Layer 2 is not activated. ISDN TEI negotiation on Layer 2 (and consequently ISDN calls on Layer 3) may fail on a Cisco 836 router when Layer 1 is active and Layer 2 is not activated.

- CSCin77315—EZVPN: crash in map_db_check_acl.

  Easy Virtual Private Network (EZVPN) crashes while reconnecting.

- CSCee66832—The **show ip access-list** command does not show configured extended access-list.

  The output of the **show ip access-list command** does not show extended access lists.

- CSCin77426—Crypto map entries not cleared for dialer, EZVPN halts at SS_OPEN.
- CSCee01865—BADSHARE tracebacks seen when packet errors occur in hardware crypto.
- CSCin82407

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

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

  This advisory will be posted to
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml

- CSCef43691

  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.

- CSCef44225

  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.

Open Caveats - Cisco IOS Release 12.2(4)YA

This section documents possible unexpected behavior by Cisco IOS Release 12.2(4)YA1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCee73477—Spurious access at show_ip2access.

  Traceback may be seen when **show ip access-list** command is given, when named access lists are configured.

  Workaround

  Use numbered access lists.

- CSCee83305—Spurious access @dialer_redial_initiate found when configured as BRI.

Additional References

The following sections describe the documentation available for the Cisco 800 and SOHO 90 Series 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 17
- Platform-Specific Documents, page 17

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Cisco IOS Release 12.2(4)YA. 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.*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 800 and SOHO 90 Series 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(4)YA, 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

Cisco IOS Software Documentation Set

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

Documentation Modules

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

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

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