Release Notes for Cisco AS5x00 Universal Gateways with Cisco IOS Release 12.4(11)XJ

March 26, 2008
Cisco IOS Release 12.4(11)XJ6
OL-14429-01 Third Release
Last Updated: September 24, 2008

These release notes describe new features and significant software components for the Cisco AS5350, Cisco AS5350XM, Cisco AS5400, Cisco AS5400HPX, Cisco AS5400XM, and Cisco AS5850-ERSC universal gateways that support the Cisco IOS Release 12.4(11)XJ 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 12.4T* located on Cisco.com.

For a list of the software caveats that apply to Cisco IOS Release 12.4(11)XJ, see the "Caveats" section on page 8 and see the online *Caveats for Cisco IOS Release 12.4T*. The caveats document is updated for every 12.4T maintenance release and is located on Cisco.com.

Contents

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

Introduction

The Cisco AS5350XM, Cisco AS5400XM, and Cisco AS5850 universal gateways are the only 1-rack unit, 2-, 4-, or 8-PRI gateway that provides universal services—data, voice, and fax services on any service, any port. The Cisco AS5350XM, Cisco AS5400XM, and Cisco AS5850 universal gateways offer high performance and high reliability in a compact, modular design. This cost-effective platform is ideally suited for Internet service providers (ISPs) and enterprises that require innovative universal services.

System Requirements

This section describes the system requirements for Cisco IOS Cisco IOS Release 12.4(11)XJ4 and includes the following sections:

Memory Requirements

Table 1, Table 2, and Table 3 describe the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Cisco IOS Release 12.4(11)XJ on the Cisco AS5350XM, Cisco AS5400XM, and Cisco AS5850 universal gateways.

Table 1 Memory Requirements for the Cisco AS5350XM Universal Gateway

Platform	Image Name	Feature Set	Software Image	Flash Memory (MB)	DRAM (MB)
AS5350XM	Cisco AS5350 Ser. IOS INT Voice/Video IPIPGW, TDMIP GW LI-mz	INT Voice/Video IPIPGW, TDMIP GW LI-mz	c5350-jk9su2_ivs-mz	128	512
	Cisco AS5350 Ser. IOS INTVoice/Video IPIPGW, TDMIP GW EPLUS	INT Voice/Video IPIPGW, TDMIP GW EPLUS	c5350-js_ivs-mz	64	512

Table 1 Memory Requirements for the Cisco AS5350XM Universal Gateway (continued)

Platform	Image Name	Feature Set	Software Image	Flash Memory (MB)	DRAM (MB)
AS5350, AS5350XM	Cisco AS5350 Ser. IOS IP Plus IPSEC 3DES	IP Plus IPSEC 3DES	c5350-ik9s-mz	64	512
	Cisco AS5350 Ser. IOS IP Plus IPSEC 3DES Lawful Intercept	IP Plus IPSEC 3DES Lawful Intercewpt	c5350-ik9su2-mz	64	512
	Cisco AS5350 Ser. IOS IP Plus	IP Plus	c5350-is-mz	64	512
	Cisco AS5350 Ser. IOS Enterprise Plus IPSEC 3DES	Enterprise Plus IPSEC 3DES	c5350-jk9s-mz	64	512
	Cisco AS5350 Ser. IOS Enterprise Plus	Enterprise Plus	c5350-js-mz	64	512

Table 2 Memory Requirements for the Cisco AS5400XM Universal Gateway

Platform	Image Name	Feature Set	Software Image	Flash Memory (MB)	DRAM (MB)
AS5400XM	Cisco AS5400 Ser. IOS INT Voice/Video IPIPGW, TDMIP GW LI	INT Voice/Video IPIPGW, TDMIP GW LI	c5400-jk9su2_ivs-mz	128	512
AS5400, AS5400HPX, AS5400XM	Cisco AS5400 Ser. IOS Enterprise Plus	Enterprise Plus	c5400-js-mz	64	512
	Cisco AS5400 Ser. IOS Enterprise IPSEC 3DES	IP Plus IPsec 3DES	c5400-jk9s-mz	64	512
	Cisco AS5400 Ser. IOS IP Plus	IOS IP Plus	c5400-is-mz	64	512
	Cisco AS5400 Ser. IOS IP Plus IPSEC 3DES Lawful Intercept	IP Plus IPSEC 3DES Lawful Intercept	c5400-ik9su2-mz	64	512
	Cisco AS5400 Ser. IOS IP Plus IPSEC 3DES	IP Plus IPSEC 3DES	c5400-ik9s-mz	64	512

Table 3 Memory Requirements for the Cisco AS5850XM Universal Gateway

Platform	Feature Set	Software Image	Flash Memory	DRAM
AS5850-ERSC	Cisco AS5850 IOS ERSC Service Provider Plus IPSEC 3DES	c5850tb-k9p9-mz	64	1024
	Cisco AS5850 IOS ERSC Service Provider Plus IPSEC3DES Lawful Intercept	c5850tb-k9p9u2-mz	64	1024
	Cisco AS5850 IOS ERSC Service Provider Plus	c5850tb-p9-mz	64	1024

Supported Hardware

Cisco IOS Cisco IOS Release 12.4(11)XJ supports the following Cisco AS5x00 platforms:

- Cisco AS5350
- Cisco AS5350XM
- Cisco AS5400
- Cisco AS5400HPX
- Cisco AS5400XM
- Cisco AS5850-ERSC

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information," page 6. 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 870 series routers, which are available on Cisco.com at the following location:

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

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

Cisco Product Documentation: **Access Servers and Access Routers**: **Access Servers**: **<platform_name>**

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5350XM, Cisco AS5400XM, and Cisco AS5850 universal gateways, log in to the router and enter the **show version** EXEC command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.4 Software (c5350-is-mz), Version 12.4(11)XJ, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, please see *How to Choose a Cisco IOS Software Release* at the following location:

http://www.cisco.com/warp/public/130/choosing_ios.shtml

For Cisco IOS Upgrade Ordering Instructions, see the document at the following location:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS and Catalyst OS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

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

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

To choose a new Cisco IOS software release based on information about defects that affect that software, use the Bug Toolkit at:

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

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 Cisco IOS Release 12.4(11)XJ supports the same feature sets as Releases 12.4 and 12.4(11)T. Cisco IOS Cisco IOS Release 12.4(11)XJ is a rebuild of Release 12.4(11)XJ 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 Triple DataEncryption Standard [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 are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and 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.

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Table 4 lists the new features and feature sets supported by the Cisco AS5350XM and Cisco AS5400XM universal gateways in Cisco IOS Cisco IOS Release 12.4(11)XJ.

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.

Table 4 New Feature List for Cisco AS5350XM and Cisco AS5400XM Universal Gateways

Feature	Software	Image
CME SIP Features	12.4(11)XJ	See Table 1, Table 2, and Table 3 for image names.
SIP REFER		
VRF-Aware H.323 and SIP for Voice Gateways		

New and Changed Information

New Hardware Features in Cisco IOS Release 12.4(11)XJ4

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XJ4

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XJ3

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XJ3

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XJ2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XJ2

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XJ

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XJ

The following new software is supported in this release:

CME SIP Features

MoH, Dialing, Line Updates, Presence with BLF, Provisioning New Phones

A presence service, as defined in RFC 2778 and RFC 2779, is a system for finding, retrieving, and distributing presence information from a source, called a presence entity (presentity), to an interested party called a watcher. When you configure presence in a Cisco Unified CME or Cisco Unified SRST system with a SIP WAN connection, a phone user, or watcher, can monitor the real-time status of another user at a directory number, the presentity.

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-roadmap.html

SIP REFER

Outside the Scope of a Dialog Created with an INVITE

Out-of-dialog REFER (OOD-R) allows remote applications to establish calls by sending a REFER message to a SIP gateway without an initial INVITE.

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-roadmap.html

VRF-Aware H.323 and SIP for Voice Gateways

VPN routing and forwarding (VRF) divides a physical router into multiple logical routers, each having its own set of interfaces and routing and forwarding tables. Adding VRF-awareness to voice gateways allows a voice gateway to exist in the same router as a customer edge (CE) or provider edge (PE) WAN router.

The VRF-Aware H.323 and SIP for Voice Gateways feature adds single voice VRF support to session-initiated protocol (SIP), H.323, and IP-to-IP gateways and to Cisco Survivable Remote Site Telephony routers. For more information, see the following link on Cisco.com:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xj11/vrfawvgw.htm

Limitations and Restrictions

There are no known limitations or restrictions in this release.

Deferrals

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Field Notices and Bulletins

For general information about the types of documents listed in this section, see the following document:

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps752/prod_field_notices_list.html

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- Product Bulletins—If you have an account on Cisco.com, you can find product bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.
- *What's Hot in Software Center—What's Hot in Software Center* provides information about caveats that are related to deferred software images. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases* at http://www.cisco.com/kobayashi/sw-center or by logging in and selecting **Technical Support > Software Center > Cisco IOS Software > What's Hot in Software Center**.
- *What's New for IOS — What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging into Cisco.com and selecting **Technical Support > Software Center > Products and Downloads > Cisco IOS Software**.

Caveats

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

Caveats in Release 12.4T are also in Cisco IOS Release 12.4(11)XJ. For information on caveats in Cisco IOS Release 12.4T, see the *Caveats for Cisco IOS Release 12.4T* document. This document lists severity 1 and 2 caveats; the documents are located on Cisco.com.

Note If you have an account on 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 **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4 > Troubleshooting > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

Open Caveats - Cisco IOS Release 12.4(11)XJ6

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ6

CSCsh12480

Cisco IOS software configured for Cisco IOS firewall Application Inspection Control (AIC) with a HTTP configured application-specific policy are vulnerable to a Denial of Service when processing a specific malformed HTTP transit packet. Successful exploitation of the vulnerability may result in a reload of the affected device.

Cisco has released free software updates that address this vulnerability.

A mitigation for this vulnerability is available. See the “Workarounds” section of the advisory for details.

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

CSCsg91306

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed 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, if administrators do not require the Cisco IOS device to provide voice over IP services.

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

Open Caveats - Cisco IOS Release 12.4(11)XJ4

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ4

Miscellaneous Caveats

- 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.

- CSCsf12082

  Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

  OSPF and MPLS VPNs are not enabled by default.

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

- CSCsk73104

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

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

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

- 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.

- CSCdv59309

  Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

  The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted.

  Cisco has made free software available to address these vulnerabilities for affected customers.

  There are no workarounds available to mitigate the effects of these vulnerabilities.

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

- CSCsj58566

  Two vulnerabilities exist in the virtual private dial-up network (VPDN) solution when Point-to-Point Tunneling Protocol (PPTP) is used in certain Cisco IOS releases prior to 12.3. PPTP is only one of the supported tunneling protocols used to tunnel PPP frames within the VPDN solution.

  The first vulnerability is a memory leak that occurs as a result of PPTP session termination. The second vulnerability may consume all interface descriptor blocks on the affected device because those devices will not reuse virtual access interfaces. If these vulnerabilities are repeatedly exploited, the memory and/or interface resources of the attacked device may be depleted.

  Cisco has made free software available to address these vulnerabilities for affected customers.

  There are no workarounds available to mitigate the effects of these vulnerabilities.

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

- CSCsg70474

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

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

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

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

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

CSCsi60004

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

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

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

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

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

CSCsi80749

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

Open Caveats - Cisco IOS Release 12.4(11)XJ3

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ3

There are no resolved caveats in this release.

Open Caveats - Cisco IOS Release 12.4(11)XJ2

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ2

CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

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-vpn.shtml.

CSCsf08998

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

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

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

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

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

CSCsd85587

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

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

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

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

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

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

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

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

Open Caveats - Cisco IOS Release 12.4(11)XJ

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ

CSCse89321: DTMF path not getting confirmed in sip media forking call

Symptom There is no end-to-end DTMF path confirmation.

Workaround There is no workaround.

CSCsf26561: User portion of Diversion header is incorrect when calling through AA

Symptom Tests on customer setup have revealed that PSTN to AA --> tx to SCCP phone--> CFWD to CUE/PSTN has an issue. The 302 Moved Temporarily from CME to BroadSoft has a Diversion header whose user portion is the private extension #, not the expanded DID # due to which the subsequent call fails.

Workaround Remove the dialplan-pattern.

CSCsf32028: Host portion of Refer-To: header must be an Address of Record

Symptom SIP trunking environments (for example, Cbeyond) need the URIs to carry Address of Record [AOR] in many SIP headers.

Workaround There is no workaround.

CSCsg17289: DNS-SRV issues for SIP registrations

Symptom Registrar, both the dial-peers would try to send a REGISTER request sequentially. When first Dial-peer (D1) is sending REGISTER Request, the registrar cache is empty. It first sends a DNS query (SRV). After getting the DNS Response, it updates the Registrar cache and sends the REGISTER request to Registrar R1. dns_count variable here is set to SIP_DNS_MODE.

When second dial-peer is sending REGISTER request, it finds the resolved IP address in registrar cache (R1) so it sends the REGISTER request to R1. dns_count variable here is set to SIP_NON_DNS_MODE. But both the REGISTER request fails as R1 is down.

As D1 is set to SIP_DNS_MODE, D1 would send a DNS query again with incremented dns_count to get any alternate Registrar and it gets R2. It sends REGISTER request to R2 and gets successfully registered. As D2 is set to SIP_NON_DNS_MODE, it does not retry the DNS query and simply backs off for period REG_EXPIRES/20.

Workaround There is no workaround.

CSCsg18902: Blind transfer is not working on SIP trunk

Symptom Blind transfer failed on SCCP endpoint over SIP trunk

Conditions When session-target is configured but outbound-proxy is not configured.

Workaround There is no workaround.

CSCsg30101:CME: dtmf-relay force rtp-nte CLI does not work

Symptom The **voice-class sip dtmf-relay force rtp-nte** command does not work.

Conditions Call comes from PSTN gw to CUE-AA, w/offer SDP of g711u, 100(NSE) CME invite's the CUE by offering g711u and NOTIFY for DTMF. CUE replies with g711u & NOTIFY for DTMF CME replies to the PSTN gw with only g711u codec with the software image.

As a result, rfc2833 is not negotiated and hence DTMF is sent raw inband. When PSTN caller presses DTMF digits after being prompted by AA, nothing works, since the CME cannot convert raw-inband DTMF to NOTIFY. With 12.4-4T3 the CME replied to the PSTN gw with g711u and rfc2833(PT=101).

Workaround There is no workaround.

CSCsg39750: Spurious mem access/traceback while resetting sip phone with presence

Solution Spurious memory access and traceback is encountered while resetting the SIP phone (7961). After configuring presence with CME.BLF speed dial entries, the status is not updated for the watched phones.

Workaround There is no workaround.

CSCsg46362: contact header incorrect in 302 message using sip-srst redirect mode

Symptom The contact header ip address is incorrect in the 302 message sent by SIP SRST in redirect mode. As the result basic call fails in this mode. B2b mode is working okay.

Workaround Use b2b mode.

CSCsg46411: CME does not send a REFER over SIP trunk for calls involving AA

Symptom CME fails to send a REFER over the SIP trunk for calls coming into the CUE-AA and being transferred to a local extension.

Conditions The CUE does a BYE-Also transfer and the CME is supposed to look at the Also: header and put that into the URI for REFER message.

Workaround There is no workaround.

CSCsg51244: CME does not send 3xx messages for transfer --> forward scenarios

Symptom CME does not send a 3xx message during call fwd if there was a call-transfer invoked before the call-forward happens.

Conditions With only **no suppl service sip refer** configured on CME at global level, we do not see the CME sending a 3xx over the SIP trunk to BSFT, Instead, a wrong reINVITE (only g711u, no dynamic payload 101) is seen when the call is forwarded to B's mailbox. This could potentially cause DTMF issues for PSTN caller. For PSTN to extension-A(DID #) CFNA to A's voicemail, the CME does send a 3xx as expected. Therefore, when a transfer is done before a forward to voicemail happens, the CME does not send a 3xx.

Workaround There is no workaround.

CSCsg51259: DTMF stops working after consult transfer to called party mailbox

Symptom PSTN connects to extension A, A transfers to B, B's CUE voicemail answers due to CFNA, A does a full consult transfer to B's CUE voicemail.

Conditions The call goes through fine, and the caller can leave a message for B, but DTMF fails even if signaling shows that 101 payload was negotiated for the SIP trunk. So if the caller wants to re-record or mark the message urgent, it does not work, although the message gets recorded.

Workaround There is no workaround.

CSCek61666: Ephone DNs get stuck in SEIZE state under certain conditions

Symptom Ephone DNs gets stuck in seize state under certain conditions, particularly under the following sequence:

1. phone-A has multiple trunk-DNs configured.
2. Call comes in on one of trunk-DN, say DN1. Call is answered and the transfer button is pressed and another extension (DN3) is dialed. The dialed extension answers the call.
3. At this time, the user on phone-A goes offhook on another trunk DN (say DN2), and dials one digit.
4. The PSTN user who is connected to DN1 hangs up and so does DN3

The above sequence gets both channels of DN1 into SEIZE state.

Conditions The rootcause of the issue was narrowed down to trunkdial flag that is part of the skinnyCB structure which is maintained per-phone. So, when DN2 goes offhook this trunkdial flag is set. When trunkdial flag in ON, all state transitions in the DN is ignored in SkinnyUpdateCallState. So, all state transitions are ignored for DN1 when the call is being cleared because the trunkdial flag is set for the entire phone rather than the specific DN.

Workaround CSCek61570 resolves this issue in the Cisco IOS 12.4(XC) throttle using a mechanism where the state transitions are not ignored it is not the active DN with trunkdial flag still in the skinnyCB structure. Make the trunkdial flag per-DN specific rather than per-phone.

`CSCek37305: Cisco 7200 router crashes at get_hwidb_if_same`

Symptom Router crashes on unconfiguring T1 controller with interface configured for RTP priority.

Conditions This is seen on 7200 NPE-G1 router loaded with 12.2(31.4.17)SB image

Workaround A workaround is to ensure that the **ip rtp priority** or **ip rtp reserve** command is removed before deleting the interface.

`CSCek39470: Router memory leak due to pak subblock chunk leaking with crypto+BVI`

Symptom Cisco IOS router running 12.4 may experience per packet memory leak due to pak subblock leak in Process memPool (not in IO mem pool). The symptom is: **show proc mem 1** output seeing the first allocator's memory count is keep growing, and never decrease.

Conditions The leak is observed with BVI (Bridge-group Virtual Interface) interface configured with crypto ipsec tunnels. Specifically when the router is doing decryption, then send the decrypted packet to BVI interface.

Workaround Shutdown any BVI (Bridge-group Virtual Interface) if being used in a router with crypto ipsec configured.

- CSCek45272: NAT overload failing with static mappings

Symptom NAT overloading from inside source address to an outside interface may fail.

Conditions The symptom was seen when translation ports were specified in an access-list associated to a route map and a second static NAT translation condition. Traffic which should have been NATed via the primary NAT overload statement failed because of the specified translation ports being used in second NAT translation condition. This occurred even though the traffic to be NATed did not meet the conditions of the second static NAT translation condition.

Workaround Remove the ip nat inside source interface X overload statement and then re-add it. The AT translations will then worked correctly until the next router reload.

- CSCek61570: Trunk dn stuck in seize/seize state and does not recover

Symptom The ephone DN may get stuck in SEIZED state and one-way audio would occur afterwards.

Conditions If another call is dropped during trunk dialing, the DN for this terminated call would move to seized state.

Workaround Press ENDCALL softkey twice to move the seized DN to idle state after finishing the and trunk call. To work around the one-way audio issue, the call needs to be transferred out and then transferred back.

- CSCek62099: MLP: PPPoE encap not applied to CEF switched non-MLP packets

Symptom When PPP Multilink is enabled over a PPP over Ethernet (PPPoE) session, outbound packets are incorrectly sent without PPPoE headers. This causes them to be dropped.

Conditions Symptom is observed in IOS version 12.4 on all software-forwarding router platforms. It only affects packets which are not multilink encapsulated (due to the bundle only having a single link).

Workaround Either disable multilink PPP, or use the ppp multilink fragment delay interface command to force multilink headers to be applied to all outbound packets.

`CSCir00074: Router crashes when casnDisconnect is set to true for pppoe session`

Symptom A router crashes when the casnDisconnect object is set to “true” for a PPPoE session.

Conditions This symptom is observed on a Cisco 10000 series when you attempt to terminate the PPPoE session through SNMP by using the casnDisconnect object of the ISCO-AAA-SESSION-MIB.

Workaround There is no workaround.

`CSCir00530: CJ-Ph2:Entry missing in cefcModuleTable for a CJ PA in Escort slot`

Symptom Entry for Crackerjack PA missing from cefcModuleTable.

Conditions SNMPGet on the table is issued.

Workaround There is no workaround.

`CSCsc48536: A router may reload unexpected due to bus error at ipnat_lock_nat`

Symptom A Cisco router may reload unexpectedly with a bus error exception.

Conditions This symptom has been observed on a router with Network Address Translation (NAT) enabled.

Workaround There is no workaround.

CSCsd50476: When channel-group configured serial interface goes down CSCse35510 OER misidentifying overlapping prefixes

Symptom A serial link goes down.

Conditions This symptom occurs when a T1/E1 controller that is configured with channel-group causes the serial link to go down. The CEM interface will not come up.

Workaround There is no workaround.

CSCse46648: IP Address Getting Removed From Interface On Deleting Crypto Config

Symptom IP address removal from a physical interface

Conditions When IPSEC connection fails and the **ip unnumbered config** is applied on the virtual template

Workaround Use cryptomaps, wit vtis, to configure the ip address on the physical interface and re attempt connection.

CSCse88584: Router proposes the default ISKMP policy if configured one does not matc

Symptom Router is proposing the default ISAKMP policy if the configured one does not match

Workaround There is no workaround.

CSCsf16536: IOSIPS - router crashes at tw_timer_start with sig action denyFlowInline

Symptom A Cisco IOS router may experience a unexpected reload.

Conditions This problem occurs when the router has IPS (Intrusion Prevention Systems) configured, and one or more attack signatures has the denyFlowInline action enabled.

Workaround Do not enable the denyFlowInline action for any IPS signatures.

CSCsf27796: 1841 router reloads at retparticle with %SYS-2-BADSHARE error

Symptom A 1841 router may reload at retparticle with %SYS-2-BADSHARE errors.

Conditions The router must be running crypto traffic using a dialer interface over a GSHDSL interface.

Workaround There is no workaround.

CSCsg02881: MLP: Bandwidth of down MLP group should be sum of member bandwidths

Symptom The bandwidth of a multilink group interface that is down does not reflect the actual bandwidths of the links that are configured as members of the multilink group. In Cisco IOS Release 12.4(8) and later, the multilink interface bandwidth reflects the bandwidth of the last link in the bundle prior to going down. In earlier versions, the bandwidth is restored to 100000 Kbps.

Conditions This symptom is observed when the multilink interface is down. The bandwidth is correct when the multilink bundle is up.

Workaround There is no workaround.

CSCsg10159: Successive Default route ctrl fails on different link but on same router

Symptom Default route withdrawn message is send from BR immediately after successful control of default roue. And prefix goes to DEFAULT state.

Conditions This only happens if OER system has only one BR and static routing protocol is used. The bug is limited to default route prefix only.

Workaround Use non-default route prefix.

CSCsg12813: Speech loss after receiving MDCX from PGW

Symptom A Cisco AS5400 gateway may change it's RTP sequence numbers after receiving a MDCX command. The RTP Stream SSRC is always the same but the Sequence Number seems to be randomly initiated again.

Conditions MGCP receives a modification request from PGW for echo cancellation 3 seconds after the call is established.

Workaround There is no workaround.

CSCsg16186: SCMabort Event crash seen on NPE-G2

Symptom System may crash during bootup.

Conditions When PA-MCX-8TE1+ is in the system and 256MB IO Memory is configured.

Workaround Reduce IO memory in the configuration.

Further Problem Description: You should see SCM Abort message in the crash info file.

CSCsg16748: ABR deletes OSPF type 3 LSA after it received max-aged type 2 LSA

Symptom In the situation ABR has both type 2 LSA and type 1 LSA for a prefix, ABR deletes type 3 LSA if it received max-aged type 2 LSA.

Workaround The workaround of this issue is configuring **timers lsa arrival** and **timers throttle lsa all** or **timers lsa-interval**.

CSCsg33172: IPS 5.0: Provide more informational error message XML and names

Symptom A few inconsistent error message.

Conditions Some SDEE messages aren't consistent with SDEE schema.

Workaround There is no workaround.

- CSCsg38907: rip - redistribute static: redistributed prefixes have metric 16

Symptom Under some conditions redistributed static routes are sent out with metric 16

Conditions * the static route for a subnet of a classfull network has a next-hop in another classfull network that is not enabled under rip. The rip update is sent out to a subnet within the same major network that the prefix of the static is about

Workaround Enable the next-hop network under rip. Configure distribute-list to filter the update.

- CSCsg39216: ezvpn tunnel traffic with **acl** keyword is not excluded from NAT

Symptom When EZVPN client is configured with "**acl**" keyword, the tunneled (vpn) traffic also gets NATed.

Conditions This only happens if there is a NAT configuration that includes the interesting VPN traffic. The tunneled traffic should be bypassed from NAT when the VPN is up.

Example:

```
crypto ipsec client ezvpn hwclient
 connect auto
 group cisco key cisco123
 mode network-extension
 peer 10.1.1.1
 acl 103
```

access-list 103 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255

This occurs when the following is true:

1) ezvpn client is configured

2) interesting tunnel traffic is defined using the "**acl**" keyword under global ezvpn configuration

3) NAT is configured

Workaround Use **crypto ipsec ezvpn client** <*ezvpn-name*> **inside** on the interface instead of **acl** keyword under ezvpn global configuration.

CSCsg39961: crash sending pki request to CA CSCsg43460 Improve NPE-G2 ENVM handling

Symptom A router may unexpectedly reload when trying to send a PKI request to a CA.

Conditions The router must be configured with crpyto PKI trustpoints.

Workaround Because this is a 1 byte redzone overrun, the following will prevent the crashes, and will display error messages instead. First, to prevent the usage of chunks, configure **no memory lite**. Second, configure **exception memory ignore overflow processor** to correct the redzone overrun.

CSCsg46546: Erroneous alerting during pickup with CSCek58324 scenario

Symptom Pickup will result in alerting from the pickup target instead of connected.

Conditions Two calls come into a trunk monitor dn. The first one to come in is answered. The second one is then answered on the same phone using the line button. Another phone uses the pickup softkey to dial the first incoming call, which is now on hold.

Workaround This issue only appears to occur on the second scenario of the above after a router reload.

CSCsg47834: NACK is observed for Open voice channel command

Symptom NACK message may be received from 5510 DSP in response to Open Voice Channel command sent by the Cisco IOS software.

```
2568288: Oct 24 13:11:33.240: //-1/xxxxxxxxxxxx/HPI/[]/hpi_tx_global_debug_info:
    DSP 3/0x3  port  INVALID_CHANNEL_STATE(85), info 0x01(1)
    DSP 3/0x00000003 port  mode CLOSED(1), state UNDEFINED(133), NACKed message
74/0x4A @0
    DSP message header 0008 0003 004A 0001 Payload: 0x0000 0x0000 0xFFFF 0x0000
```

Conditions This problem may be observed when a same 5510 DSP is used as a Transcoding and Voice Termination resource.

Workaround

1) Disable Transcoding

(or)

2) Make sure that the Transoding and Voice Termination are on different DSP(s).

This can be performed by configuring the maximum number of transcoding sessions to a value such that it would require a multiple of 240 DSP credits.

Example 1:

In the following configuration each transcoding session (complexity=high) will require 40 DSP credits. In order to use a multiple of 240 credits, we need to set the maximum transcoding sessions to 6 (6 * 40 = 240) or any multiple of 6.

```
dspfarm profile 1 transcode
 codec g711ulaw
 codec g729r8
 associate application SCCP

Router(conf-t)#dspfarm profile 1 transcode
Router(config-dspfarm-profile)#maximum sessions 6
```

Example 2:

In the following configuration each transcoding session (complexity=medium) will require 30 DSP credits. In order to use a multiple of 240 credits, we need to set the maximum transcoding sessions to 8 (8 * 30 = 240) or any multiple of 8.

```
dspfarm profile 2 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 associate application SCCP

Router(conf-t)#dspfarm profile 2 transcode
Router(config-dspfarm-profile)#maximum sessions 8
```

Use **show voice dsp group all** command to verify DSP resource allocation.

Note: Each 5510 DSP has 240 Credits. This work-around cannot be implemented if the router has only one PVDM2-16 which has only one DSP.

CSCsg48183: Unforeseen ARP request send from all interfaces

Symptom A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

Conditions This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

- Reload the router.
- A switchover of the active RP occurs.
- Enter the **redundancy force-switchover main-cpu** command.

Workaround There is no workaround.

CSCsg57228: IPS5.0: c871 reloads using IOS-S222 package file

Symptom Router crashes loading the IOS signature package file

Conditions Appeared to happen the most on the Cisco 871 and Cisco 2600 platforms.

Workaround There is no workaround.

CSCsg68199: Trunk DN offhook is not propagated to a phone already in dial out mode

Symptom Two IP Phones A and B are registered with Cisco CallManager Express; these phones share two trunk DNs 1 & 2. If Phone-A goes offhook on DN-1 and Phone-B immediately goes offhook on DN-2. This condition should show the DN-2 button on Phone-A as busy which is not happening.

Conditions This happens only when trunk DNs are used and the they go offhook in quick succession on different phones and are in dialing mode.

Workaround There is no workaround.

CSCsg68711: Incoming call in background does not audibly ring after transfer commit

Symptom Phone does not ring for the second incoming call after committing transfer at alert for the first call.

Conditions While transferring a trunk DN call, a call comes in. After committing the transfer at alert, the incoming call still doesn't ring on the phone.

Workaround There is no workaround.

CSCsg70221: DTMF through the hairpin of a trunk DN does not work

Symptom DTMF tones are being suppressed to prevent duplicate DTMF tones from being extended to an SCCP controlled VG224 port. This problem is direct result of a fix implemented for correct CSCsf98754. The lack of DTMF prevents IVR devices from working correctly

Conditions PSTN -- FXO --- CME GATEWAY --- VG224/FXS --- IVR

A call comes into a FXO port that is part of a trunk group and gets transferred to an extension that is hanging off of a vg224. DTMF is not relayed to the end point

Workaround Set the transfer system to full blind to prevent the blocking of the DTMF.

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, and 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)

CSCsg73806: Runaway debugs: AFW_Module_ObjectCount pCallIndSs

Symptom A router may display the following message to the console repeatedly:

```
AFW_Module_ObjectCount pCallIndSs 1
```

This is a cosmetic error. With the fix, this message will only be seen with debugs enabled.

Conditions This is seen on voice routers.

Workaround There is no workaround.

CSCsg78801: 4.x MinHits or 5.0 event-count not summarizing correctly

Symptom Min hit or event count not resetting correctly

Conditions Will fire signature on 1st occurrence of event, but never resets correctly so may or may not continue to fire signature.

Workaround There is no workaround.

CSCsg90212: VSA: Add code to handle CRNG failure interrupt

Symptom When VSA encounters a Continual RNG failure, the IOS will print the message

```
VSA encountered CRNG failure
```

Workaround There is no workaround.

Additional References

The following sections describe the documentation available for the Cisco AS5350XM, Cisco AS5400XM, and Cisco AS5850 universal gateways. 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 27
- Platform-Specific Documents, page 27

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Cisco IOS Cisco IOS Release 12.4(11)XJ. They are located on Cisco.com:

To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.4(11)T*, follow this path:

Technical Documents: **Cisco IOS Software**: **Release 12.4**: **Release Notes**

- To reach product bulletins, field notices, and other release-specific documents, follow this path:

  Technical Documents: **Product Bulletins**

- To reach the *Caveats for Cisco IOS Release 12.4* and *Caveats for Cisco IOS Release 12.4T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.4, follow this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.4**: **Caveats**

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco AS5350XM, Cisco AS5400XM, and Cisco AS5850 universal gateways are available on Cisco.com at the following location:

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

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

Technical Support & Documentation: Documentation: Access Servers and Access Routers: Access Servers: <platform_name>

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 access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to set up an account.

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.

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

Open Source License Acknowledgements

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

   The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

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 that are shipped with your order in electronic form.

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.