Release Notes for Cisco AS5000 Universal Gateways with Cisco IOS Release 12.4(15)XY

First Released: February 11, 2008
Last Revised: March 25, 2009
Cisco IOS Release 12.4(15)XY5
OL-15991-02 Fifth Release

These release notes describe new features and significant software components for the Cisco 5000 series routers that support Cisco IOS Release 12.4(15)XY. These release notes are updated as needed. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* and *About Cisco IOS Release Notes*.

For a list of the software caveats that apply to Cisco IOS Release 12.4(15)XY, see the "Caveats" section on page 7 and see the online *Caveats for Cisco IOS Release 12.4(15)T*. The caveats document is updated for every 12.4T maintenance release.

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 Release 12.4(15)XY and includes the following sections:

Memory Requirements

Table 1and Table 2 describe the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 12.4(15)XY on the Cisco AS5350XM, Cisco AS5400XM, and Cisco AS5850 universal gateways.

Table 1 Memory Requirements for the Cisco AS5350XM Universal Gateway

Platform	Feature Set	Software Image	Flash Memory (MB)	DRAM (MB)
Cisco AS5350XM	c5350-jk9su2_ivs-mz	Cisco AS5350 Ser. IOS INT Voice/Video IPIPGW, TDMIP GW LI	64	512
	c5350-js_ivs-mz	Cisco AS5350 Ser. IOS INT Voice/Video IPIPGW, TDMIP GW EPLUS	128	512
Cisco AS5350	Cisco AS5350 IOS IP PLUS IPSEC 3DES	c5350-ik9s-mz	64	256
	Cisco AS5350 IOS IP PLUS IPSEC 3DES LAWFUL INTERCEPT	c5350-ik9su2-mz	64	256
	Cisco AS5350 IOS IP PLUS	c5350-is-mz	64	256
	Cisco AS5350 IOS ENTERPRISE PLUS IPSEC 3DES	c5350-jk9s-mz	64	256
	Cisco AS5350 IOS ENTERPRISE PLUS	c5350-js-mz	64	256

Table 2 Memory Requirements for the Cisco AS5400XM Universal Gateway

Platform	Feature Set	Software Image	Flash Memory (MB)	DRAM (MB)
Cisco AS5400XM	Cisco AS5400 IOS IP PLUS IPSEC 3DES	c5400-ik9s-mz	64	512
	Cisco AS5400 Ser. IOS INT Voice/Video IPIPGW, TDMIP GW LI	c5400-jk9su2_ivs-mz	64	512
	Cisco AS5400 Ser. IOS INT Voice/Video IPIPGW, TDMIP GW EPLUS	c5400-js_ivs-mz	128	512
Cisco AS5400, AS5400HPX,	Cisco AS5400 IOS IP PLUS IPSEC 3DES	c5400-ik9s-mz	64	128
	Cisco AS5400 IOS IP PLUS IPSEC 3DES LAWFUL INTERCEPT	c5400-ik9su2-mz	64	128
	Cisco AS5400 IOS IP PLUS	c5400-is-mz	64	128
	Cisco AS5400 IOS ENTERPRISE PLUS IPSEC 3DES	c5400-jk9s-mz	64	128
	Cisco AS5400 IOS ENTERPRISE PLUS	c5400-js-mz	64	128
Cisco AS5850-ERSC	Cisco AS5850 IOS ERSC SERVICE PROVIDER PLUS IPSEC 3DES	c5850tb-k9p9-mz	64	1G
	Cisco AS5850 IOS ERSC SP PLUS IPSEC3DES LAWFUL INTERCEPT	c5850tb-k9p9u2-mz	64	1G

Supported Hardware

Cisco IOS Release 12.4(15)XY supports the following Cisco AS5000 platforms:

- Cisco AS5350
- Cisco AS5350XM
- Cisco AS5400
- Cisco AS5400XM

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 4. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco AS5000 series routers at:

http://www.cisco.com/web/psa/products/index.html?c=268437594

Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco AS5000 series router, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Feature Set Tables

For information about Feature Set Tables, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

New and Changed Information

New Hardware Features in Cisco IOS Release 12.4(15)XY5

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY5

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XY4

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY4

The are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XY3

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY3

The are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XY2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY2

The are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(15)XY1

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY1

The new software features are:

- Transparent Tunneling of QSIG over SIP-TDM Gateway, page 5
- SIP SRTP fallback to non-secure RTP, page 6
- Pass data in SIP REFER to triggered INVITE, control media-cut through on SIP 18x response, page 6

Transparent Tunneling of QSIG over SIP-TDM Gateway

The “Transparent Tunneling of QSIG over SIP-TDM Gateway” feature provides transparent transport of QSIG-protocol ISDN messages across the SIP trunk. In 12.4(15)XY1, this solution is supported only for QSIG protocol messages, unlike H.323 gateways, which tunnel any raw message. This solution encapsulates QSIG messages within SIP message bodies using application/qsig MIME to tunnel between SIP endpoints. This solution does not add any QSIG services to SIP interworking.

In 2.4(15)XY1, QSIG tunneling is supported only on SIP-TDM gateways with ISDN PRI or BRI. So Cisco Unified Border Element (Cisco UBE), formerly known as the Cisco IOS Session Border Controller (SBC) or the Cisco Multiservice IP-to-IP Gateway, cannot yet utilise this feature.

SIP SRTP fallback to non-secure RTP

The "SIP SRTP fallback to non-secure RTP" feature provides compatibility with Cisco Unified Communications Manager, version 7.0. SRTP fallback to RTP was previously supported between two gateways. Now, with a new negotiation method introduced in 12.4(15)XY1, support for this feature is provided between the gateways and the Cisco Unified Communications Manager.

Pass data in SIP REFER to triggered INVITE, control media-cut through on SIP 18x response

The control media-cut through on SIP 18x response feature provides the ability to send media backward even before the call is established. So instead of allowing media to flow both ways only after the call is established, this feature allows the remote side to send a personalized ringback tone (usually music) as a response even before the call is established.

Doing only backward media cut-through on 18x messages affects the digit collection process (RFC 2833 mechanism) before the call is connected (SIP 200 OK message is sent and accepted). Since most of the SIP IVR deployments use RFC 2833 to collect digits before a call is connected, the current default behavior (bidirectional media cut-through on 18x) is retained.

The Pass data in SIP REFER to triggered INVITE feature provides the ability to map SIP REFER message data into SIP INVITE messages. This new feature allows you to send customer-specific information to triggered SIP INVITE messages using Call-Info as the URL header of the SIP REFER-TO message. Further, this feature allows the gateway to take SIP REFER data and create a new SIP INVITE message to a new destination when a call is being placed to an Interactive Voice Response (IVR) endpoint and the IVR refers the call to an agent or to another IVR system.

New Hardware Features in Cisco IOS Release 12.4(15)XY

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(15)XY

The following new software is supported in this release:

- AMR-NB and iLBC Codec Support for MGCP, page 6
- DSP Voice Quality Metrics, page 7
- Universal Voice Transcoding Support for IP-to-IP Gateways, page 7

AMR-NB and iLBC Codec Support for MGCP

The Adaptive Multirate Narrow Band (AMR-NB) codec is a high complexity multimode codec that adapts to speech and channel coding depending on channel conditions. The internet Low Bitrate Codec (iLBC) is a standard, high-complexity speech codec that is suitable for robust voice communication over IP. These codecs are now available for use with MGCP.

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/it_amrnb.html

DSP Voice Quality Metrics

DSP voice quality metrics improve your ability to monitor, analyze, and ultimately meet your quality of service (QoS) objectives for your network. For more information, go to:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/vqmetric.html

Universal Voice Transcoding Support for IP-to-IP Gateways

Universal Transcoding allows transcoding from any supported codec to any other supported codec. For more information, go to:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/it_unitr.html

New Features in Release 12.4T

For information regarding the features supported in Cisco IOS Release 12.4T, see the Cross-Platform Release Notes links at: http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html

Limitations and Restrictions

There are no known limitations or restrictions in this release.

Caveats

For general information on caveats and the bug toolkit, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

This section contains the following caveat information:

Open Caveats - Cisco IOS Release 12.4(15)XY5

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(15)XY5

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website 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-20090908-tcp24.shtml.

CSCsm97220

Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at the following link
http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml

CSCsr29468

Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

Cisco has released free software updates that address this vulnerability.

Several mitigation strategies are outlined in the workarounds section of this advisory.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

CSCso04657

Symptom SSLVPN service stops accepting any new SSLVPN connections.

Conditions A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

CSCsk40676 C1812 12.4.15.T / certain pkt size block inside interface of ezvpn conn.

Symptom The inside interface of a Cisco router running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

Conditions Occurs when LZS compression is used on a Windows Vista client.

Workaround Disable LZS compression.

CSCse85652 HTTP should deny access if no enable password is configured.

CSCsg04630 7600BB: DHCP:STB crash MEM corruption at dhcpd_add_binding_to_radix_tree.

CSCsj87522 AS5350 hung calls or socket leak causes IPIPGW to run out of rtp ports.

Symptom RTP and RTCP ports are leaked when a ReleaseComplete (reason=newConnectionNeeded) is received as a response to a FastStart Setup that is sent.

Conditions This problem is seen in Cisco IOS Release 12.4(11)T and Release 12.4(15)T images for a normal H323 to H323 gatekeeper routed call with no supplementary services.

Workaround There is no workaround.

CSCsk32970 ccm switchover fails as ACL does not deny properly.

Symptom Alternative packets are not being dropped by Extended ACL with deny statements in cef switching path.

Conditions When CEF is enabled.

Workaround Disable CEF or use standard ACL.

CSCsk58014 Module fails to boot up after reset.

Symptom The module will not return to the steady state after a reset.

Conditions This symptom is observed whenever the module is reset.

Workaround There is no workaround.

CSCsk61991 dsl controller with auto linemode is down with peer in 4-wire linemode.

Symptom Ping failure is seen over ATM interface in 4-wire line mode as the ATM interface does not come up.

Conditions With the UUT configured as auto the ATM interface continues to be down after the peer changes from 2-wire to 4-wire enhanced. This happens only on WIC-1SHDSL with UUT configured as auto which is not recommended.

Workaround Do not configure the line mode as auto.

CSCsk63655 MGCP gateway returns 524 instead of 200 for a valid LCO param in CRCX.

Symptom A Media Gateway Control Protocol (MGCP) gateway may return a 524 or 510 error code with the reason as "invalid local connection option" for a valid "L:" parameter in a CRCX message.

Conditions The symptoms can be observed on a router that is running Cisco IOS Interim Release 12.4(17.4)T1 or later, when the **<CmdBold>debug mgcp parser<noCmdBold>** command with verbose tracelevel is disabled.

Workaround Enable **<CmdBold>debug mgcp parser<noCmdBold>** with verbose tracelevel.

CSCsk70060 crafted packets to UDP port 2887 with AP HWIC may cause queue wedge.

Symptom Crafted packets to UDP port 2887 with AP HWIC may cause queue wedge.

Conditions The router must have AP HWIC installed, and UDP port 2887open.

Workaround None.

CSCsk92135 UUT with ADSL over POTS card goes to hang state while booting IOS.

Symptom Routers with ADSL over POTS card hang on booting Cisco IOS Release 12.4(16.14)T4 and above.

Conditions Issue seems to be specific to the ADSL over POTS card.

Workaround There is no workaround.

CSCsk93241 Chunk memory corruption on LFDp Input Proc.

Cisco IOS Software Multi Protocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected. Cisco has released free software updates that address this vulnerability.

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml

CSCsl04399 PRI FAX calls failing for E1 controller.

Symptom Fax call is aborted while testing PRI E1 feature.

Conditions Occurs in routers running a pre-release version of Cisco IOS Release 12.4(15)T2.

Workaround Use the **<CmdBold>fax rate disable<noCmdBold>** command to disable the fax relay feature under the VoIP dialpeer.

CSCsl22080 12.4.15T: WebVPN stops working with TCP connection queue limit reached.

Symptom WebVPN hangs after a few days of working. When this happens, no WebVPN connections are active and no new connections can be established. The **<CmdBold>debug ip tcp transaction<noCmdBold>** command shows <CmdBold>connection queue limit reached: port 443<noCmdBold> errors. The **<CmdBold>show tcp brief<noCmdBold>** command displays many sessions in SYNRCVD and TIMEWAIT states. Problem is recovered either by reload or by entering the **<CmdBold>clear tcp tcb *<noCmdBold>** command. There are few stale sessions in CLOSED state left after clearing TCP.

Conditions Issue seen in Cisco IOS Release 12.4.15T and Cisco IOS Release 12.4.15T1 when WebVPN is configured. The issue is intermittent and happens after a few days or weeks of working.

Workaround To restore TCP connectivity, issue **<CmdBold>clear tcp tcb *<noCmdBold>** or reload the router. Note that this will clear all TCP sessions on the router.

CSCsm45113 RIB installs duplicate routes for the same prefix.

Symptom Router may install duplicate routes or incorrect route netmask into routing table. It could happen on any routing protocol. Additionally, for OSPF, crash was observed.

Conditions The problem is triggered by SNMP polling of ipRouteTable MIB. The problem is introduced by CSCsj50773, see the Integrated-in field of CSCsj50773 for affected images.

Workaround Do not poll ipRouteTable MIB, poll newer replacement ipForward MIB, instead. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

Further Problem Description: The **<CmdBold>clear ip route *<noCmdBold>** command can correct the routing table until the next poll of ipRouteTable MIB.

CSCso18940 snmpwalk on 'ipRouteTable' returns error - OID not increasing.

CSCso60174 Multiple duplicate descriptions found for mmoip aaa commands.

CSCsq15993 PBR is not supported in CEF switching path on 12.4(15)XY release

CSCsr15478 Input Queue Wedging.

Symptom An input wedge is observed on an interface, when multicast traffic is flowing.

Conditions The symptom is observed in a DMVPN hub-spoke scenario with a point-to-multipoint (P2MP) GRE tunnel having tunnel protection configuration. When multicast traffic flows from hub to spoke through these tunnel interfaces, the incoming interface of the hub is getting wedged and even the ping to peer stops working.

Workaround There is no workaround, other than reloading the router.

CSCsu64215 ip tcp adjust-mss command results in packet loss for non-TCP traffic.

Open Caveats - Cisco IOS Release 12.4(15)XY4

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(15)XY4

- CSCsq58779

  Cisco IOS devices that are configured for Cisco Unified Communications Manager Express (CME) and the Extension Mobility feature are vulnerable to a buffer overflow vulnerability. Successful exploitation of this vulnerability may result in the execution of arbitrary code or a Denial of Service (DoS) condition on an affected device.

  Cisco has released free software updates that address this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-cme.shtml

CSCso56129 %SYS-2-BADSHARE: Bad refcount in datagram_done monitoring cme/cue calls

Symptom Bad Refcount is seen with tracebacks.

Conditions Using AIM-IPS-K9 to monitor interfaces with ephones registered to the CME on the same router and have ephone check voice mail. This is in a branch in a box setup. UUT serves as a CME as well as having the voice mail AIM in the same router.

Workaround There is no workaround.

CSCso66843 CUBE and CME do not change embedded SSRC in RTCP packets

Symptom Different SSRC in RTCP compared to RTP after transcoding.

Conditions Voice call with transcoding in CUBE or CME.For a voice call passing through transcoding on CUBE or CME, the SSRC value contained within the RTCP is passed unchanged, whereas the SSRC value contained within the RTP is changed. This creates a mismatch between the SSRC between RTP and RTCP at the final destination.

Workaround There is no workaround.

CSCso67655 S2 CFD: Secure DSPFarm doesn't register after a reload of the router

Symptom After Reolad Secure Conference profile does not register with CCM.

Conditions This happens when a specific trustpoint is specified for CCM cert authentication during TLS handshake.

Workaround The workaround is not to specify the truspoint when configuring callmanger CCM using CLI "sccp ccm <ip address> tag version <x>.

CSCsq44013 View used twice with logging enabled

Symptom The CPE does not reply to the DNS query from the client for the first try, first response is being dropped.

Conditions This is seen on a router running 12.4T IOS image configured with split DNS.

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 12.4(15)XY3

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(15)XY3

CSCsk62253

Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

CSCsk42759

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.

CSCsl62609

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.

CSCso81854

Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml.

This security advisory is being published simultaneously with announcements from other affected organizations.

CSCsk42419

Symptom The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

The Security Advisory for this issue is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml

CSCsk60020

Symptom The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug. The Security Advisory for this issue is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml.

CSCsk29999 AIM-IPS-K9:TCP intercept not entering aggressive mode

Symptom When configuring the AIM-IPS-K9 with tcp intercept, the tcp intercept may not enter aggressive mode. Traffic is not impacted.

Conditions When the performance level of passing packets to the IPS application is below the window size at which the IPS application enters aggressive mode, it will not enter aggressive mode. On low-end platforms where the router is a constrictor on traffic sent to the card, this problem may be more pronounced.

Workaround Do not configure tcp intercept with AMI-IPS-K9.

CSCsl61734 CUBE slow start h323 to sip transfer = dead air

Symptom Slow start H323 to SIP calls may experience no-way audio if the call is transferred after initially connected.

Conditions This only occurs with slow start H323.

Workaround Use fast start H323.

CSCsl68798%SYS-2-PAK_SUBBLOCK_SETSIZE traceback at control_plane_init() at boot

Symptom At boot-time an IOS device may generate tracebacks of the form:

```
*Mar 1 00:00:10.339:%SYS-2-PAK_SUBBLOCK_SETSIZE: 28 -Process= "Init", ipl= 3, pid= 3,
-Traceback= 0x601597F4 0x60260E80 0x602C3928 0x6014E588 0x6014E7E4 0x6028B680 0x6028B664
```

Conditions This behaviour is observed on an IOS device installed with 12.5(0.5) or later or 12.4(15)XY IOS releases.

Workaround There is no known workaround.

CSCsl88956 Primary nvram is not properly restored after it is corrupted

Symptom when the Cisco 28xx and 38xx routers is reloaded, they loose the running configuration and startup configuration.

Conditions If the last physical sector of nvram which is shared by nvram and licensing subsystem is corrupted, primary nvram is not restored properly.

Workaround There is no known workaround.

Open Caveats - Cisco IOS Release 12.4(15)XY2

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(15)XY2

CSCsi01875 IPIP gateway rejects a second TCS

Symptom Placing a video call from a Polycom device. The call gets rejected because Polycom sends a TCS before receiving the TCS ACK.

Conditions Polycom video endpoints and IP gateway.

Workaround There is no workaround.

CSCse60897 call-manager-fallback does not allow more than 5 redirects

Symptom After 5 redirects, calls fail with busy tone when in call-manager-fallback.

Conditions The maximum redirects seem to be 5 only.

Workaround There is no workaround.

CSCsk09472 printf_ptr warnings still exist after CSCsj92597

Symptom The printf_ptr warnings that would appear during a build of the obj-m8500-c1800/c180x-broadband-mz no longer appear.

Workaround Moving the define for printf_ptr to another file solved the issue.

CSCsl70220 Entity hierarchy issue in 1805 device

Symptom The root entity is pointing to modem card instead of chassis.

Conditions It will affect SNMP based management application like CiscoView.

Workaround There is no workaround.

CSCsl72097 Alignment Error seen in 3800 while making E1/r2 call.

Symptom While making E1/r2 calls alignment tracebacks were seen. The traceback reported where for alignment corrections.

Conditions The alignment errors were seen as we were accessing (writing into) non-aligned address.

Workaround Write using PUTLONG which will do a 4-byte write on un-aligned memory will fix this issue.

CSCsm34933 Refresh Re-Invite disconnect call because CUBE does not send out 200 OK

Symptom In 12.4(15)XY, when cube receives the session refresh re-invite with sdp then it sends 100 trying but no 200 OK and therefore call gets dropped.

Conditions Call gets dropped since no 200 OK sent by CUBE

Workaround There is no workaround.

CSCsm44512 Router crash when unconfigure PVC from ATM interface

Symptom Router might crash if unconfig the PVC from ATM interface without shutting down the interface first.

Conditions Crash only observed when interface was up before the PVC removal.

Workaround Shut down the ATM interface first before the PVC removal.

CSCsm44792 input gain auto-control -9 is added automatically to voice-ports.

Symptom The command is added automatically to the voice-port configuration: input gain auto-control -9. In addition, this command can not be removed by the "no input gain auto-control -9". This issue causes voice issues to the VTG in the IPICS system.

Conditions This issue is seen after upgrading router from 12.4(6)T6 or 12.5(15)T1 to 12.(4)15XY.

Workaround No known workaround.

This is a sample configuration of the voice port: voice-port 0/2/0:0 voice-class permanent 1 auto-cut-through lmr m-lead audio-gate-in lmr e-lead voice input gain auto-control -9 no echo-cancel enable playout-delay nominal 100 playout-delay minimum high no comfort-noise timeouts call-disconnect 3 timeouts tear down lmr infinity timing hookflash-in 0 timing hangover 40 connection trunk 19990929090 description #0/2/0:0#0# INUSE 1221.

Open Caveats - Release 12.4(15)XY1

CSCsl22920 - IOS gw not tunneling ISDN ALERTING message over SIP

Symptom ISDN QSIG ALERTING message received from Destination PINX is not transparently transported to Originating PINX.

Conditions This is seen if the Destination PINX sends ISDN QSIG CALL_PROC with PI==1 in response to ISDN QSIG SETUP message.

Workaround There is no workaround.

Further Problem Description: ISDN QSIG CALL_PROC with PI==1 received from destination PINX is converted to SIP 183 Progress at TGW and hence treated as ISDN QSIG PROGRESS at OGW/Originating PINX. Due to this 183 corresponding to ISDN QSIG ALERTING from Dest PINX is dropped at OGW.

Resolved Caveats - Release 12.4(15)XY1

There are no resolved caveats in this release.

Open Caveats - Cisco IOS Release 12.4(15)XY

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(15)XY

CSCsj85065

A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

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

CSCsi53006 Router crash in cmm_crs_proc_tr_call_trans_req

Symptom CME with UCCX integration could crash at the following function:

```
cmm_crs_proc_tr_call_trans_req()
```

Conditions The crash would only occur in very rare condition. Indeed the problem is difficult to reproduce. This could happen when an sccp endpoint attempts a consult transfer.

Workaround There is no workaround.

CSCsi69819 Line protocol down when no auto speed and duplex negotiate on onboard FE

Additional References

Use this release note with the documents and websites in this release note and the documents listed in the following sections:

- Release-Specific Documents, page 22
- Platform-Specific Documents, page 22

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.4(15)XY.

- *Cross-Platform Release Notes for Cisco IOS Release 12.4)T*
- *Cisco IOS Software Releases 12.4 Special and Early Deployments*
- *Caveats for Cisco IOS Release 12.4(15)T*

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 at:

http://www.cisco.com/web/psa/products/index.html?c=268437594

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.

Notices

See the "Notices" section in *About Cisco IOS Release Notes* located at: http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

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