Release Notes for Cisco 2691 and Cisco 2600XM Series Routers with Cisco IOS Release 12.4(4)XC

June 9, 2008
Cisco IOS Release 12.4(4)XC7
OL-9576-02 Seventh Release
Last Revised: September 24, 2008

These release notes describe new features and significant software components for the Cisco 2691 and Cisco 2600XM series routers that support the Cisco IOS Release 12.4(4)XC releases. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. For a list of the software caveats that apply to Release 12.4(4)XC, see the "Caveats" section on page 10 and *Caveats for Cisco IOS Release 12.4(4)T*. The online caveats document is updated for every maintenance release.

Contents

System Requirements

This section describes the system requirements for Release 12.4(4)XC and includes the following sections:

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

Memory Requirements

Table 1 describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Cisco IOS Release 12.4(11)XJ on the Cisco 2691 and Cisco 2600XM series routers.

Table 1 Required Memory for the Cisco 2691 and Cisco 2600XM Series Routers with Cisco IOS Release 12.4(4)XC

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
2610XM 2611XM 2620XM 2621XM 2650XM 2651XM	Cisco 2600 IPV-AESK9 Feature Set Factory Upgrade For Bundles Cisco 2600 AISK9-AESK9 Feature Set Factory Upgrade For Bundles Cisco 2600 SPSK9-AESK9 Feature Set Factory Upg For Bundles	Feat Set Factory Upgrade For Bundles	c2600-adventerprisek9-mz	48	256
	Cisco 2600 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES	INT VOICE/VIDEO, IPIPGW, TDMIP GW AES	c2600-adventerprisek9_ivs-mz	64	256
	Cisco 2600 Advanced Enterprise Services With SNA Switch	Advanced Enterprise Services With SNA Switch	c2600-adventerprisek9_sna-mz	48	256
	Cisco 2600 Advanced IP Services Cisco 2600 IPV-AISK9 Feature Set Factory Upgrade For Bundles Cisco 2600 SPSK9-AISK9 Feature Set Factory Upgrade For Bundles	Advanced IP Services Feature Set Factory Upgrade For Bundles	c2600-advipservicesk9-mz	48	192
	Cisco 2600 Advanced Security	Advanced Security	c2600-advsecurityk9-mz	32	128
	Cisco 2600 Enterprise Base w/o Crypto	Enterprise Base w/o Crypto	c2600-entbase-mz	32	128
	Cisco 2600 Enterprise Base	Enterprise Base	c2600-entbasek9-mz	32	128
	Cisco 2600 Enterprise Services w/o Crypto	Enterprise Services w/o Crypto	c2600-entservices-mz	48	192

Table 1 Required Memory for the Cisco 2691 and Cisco 2600XM Series Routers with Cisco IOS Release 12.4(4)XC

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
	Cisco 2600 Enterprise Services Cisco 2600 IPV-ESK9 Feature Set Factory Upg For Bundles Cisco 2600 SPSK9-ESK9 Feature Set Factory Upg For Bundles	Enterprise Services Feature Set Factory Upgrade For Bundles	c2600-entservicesk9-mz	48	192
	Cisco 2600 IP Base w/o Crypto	IP Base w/o Crypto	c2600-ipbase-mz	32	128
	Cisco 2600 IP Base	IP Base	c2600-ipbasek9-mz	32	128
	Cisco 2600 IP VOICE W/O CRYPTO	IP Voice w/o Crypto	c2600-ipvoice-mz	48	192
	Cisco 2600 INT VOICE/VIDEO, IPIP GW, TDMIP GW	INT VOICE/VIDEO, IPIP GW, TDMIP GW	c2600-ipvoice_ivs-mz	64	256
	Cisco 2600 IP Voice	IP Voice	c2600-ipvoicek9-mz	48	192
	Cisco 2600 SP Services Cisco 2600 IPV-SPSK9 Feature Set Factory Upg For Bundles	SP Services Feature Set Factory Upgrade For Bundles	c2600-spservicesk9-mz	48	192

Table 1 Required Memory for the Cisco 2691 and Cisco 2600XM Series Routers with Cisco IOS Release 12.4(4)XC

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
2691	Cisco 2691 Advanced Enterprise Services	Advanced Enterprise Services	c2691-adventerprisek9-mz	64	256
	Cisco 2691 INT Voice/Video, IPIPGW, TDMIP GW AES	INT Voice/Video, IPIPGW, TDMIP GW AES	c2691-adventerprisek9_ivs-mz	64	256
	Cisco 2691 Advanced Enterprise Services With SNA Switching	Advanced Enterprise Services With SNA Switching	c2691-adventerprisek9_sna-mz	64	256
	Cisco 2691 Advanced IP Services	Advanced IP Services	c2691-advipservicesk9-mz	64	256
	Cisco 2691 Advanced Security	Advanced Security	c2691-advsecurityk9-mz	64	256
	Cisco 2691 Enterprise Base w/o Crypto	Enterprise Base w/o Crypto	c2691-entbase-mz	64	256
	Cisco 2691 Enterprise Base	Enterprise Base	c2691-entbasek9-mz	64	256
	Cisco 2691 Enterprise Services w/o Crypto	Enterprise Services w/o Crypto	c2691-entservices-mz	64	256
	Cisco 2691 Enterprise Services	Enterprise Services	c2691-entservicesk9-mz	64	256
	Cisco 2691 IP Base w/o Crypto	IP Base w/o Crypto	c2691-ipbase-mz	32	128
	Cisco 2691 IP Base	IP Base	c2691-ipbasek9-mz	32	128
	Cisco 2691 IP Voice w/o Crypto	IP Voice w/o Crypto	c2691-ipvoice-mz	64	256
	Cisco 2691 INT Voice/Video, IPIP GW, TDMIP GW	INT Voice/Video, IPIP GW, TDMIP GW	c2691-ipvoice_ivs-mz	64	256
	Cisco 2691 IP VOICE	IP Voice	c2691-ipvoicek9-mz	64	256
	Cisco 2691 SP Services	SP Services	c2691-spservicesk9-mz	64	256

Hardware Supported

Cisco IOS Release 12.4(4)XC supports the Cisco 2691 and Cisco 2600XM series routers.

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 2691 and Cisco 2600XM series routers, which are available on Cisco.com and the Documentation CD at the following location:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/2600/index.htm

Determining the Software Version

To determine which version of Cisco IOS software is currently running on your Cisco 2691 or Cisco 2600XM series router, log in to the router and enter the **show version** privileged EXEC command. The following sample output from the **show version** command indicates the version number.

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C2691 Software (C2691-Y7-MZ), Version 12.4(11)XJ, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.4(4)T
```

Upgrading to a New Software Release

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

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.4(4)XC supports the same feature sets as Releases 12.4 and 12.4(4)T, but Release 12.4(4)XC includes new features supported by the Cisco 2691 and Cisco 2600XM series routers.

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

Table 2 lists the feature and feature sets supported in Cisco IOS Release 12.4(4)XC

The tables use the following conventions:

- In—The number in the ‘In’ column indicates the Cisco IOS release in which the feature was introduced. For example, “12.4(4)XC” indicates that the feature was introduced in 12.4(4)XC. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.

Note These feature set tables contain only a selected list of features, which are cumulative for Release 12.4(4)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in *Cross-Platform Release Notes for Cisco IOS Release 12.4(4)T* and Release 12.4(4)T Cisco IOS documentation.

Table 2 Cisco IOS Release 12.4(4)XC Feature List for Cisco 2691 and Cisco 2600XM Series Routers

Feature	In	Image
Call Detail Records (CDR) Feature Correlation ID for Supplementary Features	12.4(4)XC	See Table 1 for image names.
Cisco Unified CallManager Express 4.0		
Cisco Unified Survivable Remote Site Telephony 4.0		
Customizable PSTN Tones and H.323 Call-Disconnect Cause Codes		
H.323 VoIP Call Preservation Enhancements for WAN Link Failures		
Integrated Services		
Video Support for SCCP-Based Endpoints		
Cisco Unified CME 4.0(4) Extension Assigner		

New and Changed Information

This section contains the following information:

Updated Naming Conventions

The following product names have been changed in Cisco IOS Release 12.4(4)XC:

- Cisco CallManager Express (Cisco CME) is now Cisco Unified CME. This change is effective in Cisco Unified CME version 4.0 and later releases.
- Cisco Survivable Remote Site Telephony (Cisco SRST) is now Cisco Unified SRST. This change is effective in Cisco Unified SRST version 4.0 and later releases.

New Software Features in Release 12.4(4)XC4

Cisco Unified CME 4.0(4) Extension Assigner

The Cisco Unified CallManager Express (CME) feature enables installation technicians to assign extension numbers to Cisco Unified CME phones without accessing the server. For more information, see the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/voice/its/cme40/cme403/extasgnr.htm

New Software Features in Release 12.4(4)XC1

New features are available for Cisco Unified CallManager Express (Cisco Unified CME), including the following:

- FXO trunk enhancements—Supports shared lines, transfer recall for transferred and forwarded calls, status monitoring of FXO ports, and line button optimization for call transfer.
- Automatic line selection enhancement—Enables automatic line selection for incoming calls on the line associated with a specified button.
- Night service ring enhancement—Overrides silent ringing during active night service periods.

For more information, see the "Cisco Unified CallManager Express 4.0" section on page 7 and the *Cisco Unified CallManager Express 4.0.1 New Features* document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xc4/cme401tk.htm

New Hardware Features in Release 12.4(4)XC

There are no new hardware features in this release.

New Software Features in Release 12.4(4)XC

The following new software features are supported by the Cisco 2691 and Cisco 2600XM series routers in Cisco IOS Release 12.4(4)XC:

Call Detail Records (CDR) Feature Correlation ID for Supplementary Features

This feature captures additional information in CDRs for voice calls that are transferred or forwarded on phones controlled by Cisco Unified CallManager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST). It includes a unique correlation ID that identifies a given call feature across all legs in a call. CDR information can be output in RADIUS VSAs or system log (syslog) messages. For more information about this feature, go to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm

Cisco Unified CallManager Express 4.0

Cisco Unified CallManager Express 4.0 (Cisco Unified CME 4.0) delivers a number of next-generation telephony features that expand system capabilities and provide key productivity enhancements.

With this release, the product name has been changed to Cisco Unified CallManager Express to underscore its position as a member of the Cisco Unified Communications family of products.

New features and expanded capabilities are introduced in the following areas:

- Basic Automatic Call Distribution (B-ACD) and Auto-Attendant (AA) Service
- Direct Inward Dial Digit Translation Service, which provides a number transformation service for DID calls
- Call forwarding, call park, call transfer, and conferencing
- Ephone hunt groups, including dynamic membership and agent status control
- Ephone templates and ephone-dn templates to apply features quickly to phones and lines
- Phone support for remote teleworkers, Cisco IP Communicator, and the newest Cisco Unified IP phones:
  - Cisco Unified IP Phone 7911G
  - Cisco Unified IP Phone 7941G
  - Cisco Unified IP Phone 7941G-GE
  - Cisco Unified IP Phone 7961G
  - Cisco Unified IP Phone 7961G-GE
- IP phone authentication for secure Skinny Client Control Protocol (SCCP) signaling between Cisco Unified CME and IP phones
- Fax passthrough mode using Cisco VG 224 voice gateways, Analog Telephone Adaptors (ATA), and SCCP
- Video support
- QSIG integration with TDM PBXs
- Feature access codes and feature control
- Redundant Cisco Unified CME router

For details about new features, see the “Feature History” chapter of the Cisco Unified CallManager Express System Administrator Guide at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_configuration_guide_book09186a00805f262e.html

For links to all Cisco Unified CallManager Express documents, see the documentation roadmap at the following URL:
http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html

Cisco Unified Survivable Remote Site Telephony 4.0

Cisco Unified Survivable Remote Site Telephony (SRST) 4.0 adds these features to the Cisco 2691 and Cisco 2600XM series routers in Cisco IOS Release 12.4(4)XC:

- Support for the following Cisco Unified IP Phone models:
  - Cisco Unified IP Phone 7911G
  - Cisco Unified IP Phone 7941G
  - Cisco Unified IP Phone 7941G-GE
  - Cisco Unified IP Phone 7961G

  - Cisco Unified IP Phone 7961G-GE
- Cisco IP Communicator support
- Fax pass-though for ATA and Cisco VG 224 and Cisco VG 248 using SCCP mode.
- H.323 VoIP call preservation enhancements for WAN link failures
- Video support

For more information about these features, go to http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_configuration_guide_chapter09186a00805fccb7.html.

Customizable PSTN Tones and H.323 Call-Disconnect Cause Codes

The Customizable PSTN Tones and H.323 Call-Disconnect Cause Codes featurette enables you to customize PSTN tones and H.323 call-disconnect cause codes for certain disconnect scenarios. Specifically, you can customize the following:

- PSTN tones that are applicable to foreign-exchange-station (FXS), PRI, and BRI calls and IP phones
- Q.850 call-disconnect cause codes for H.323 gateways

In addition, you can specify the mechanism for detecting media inactivity (silence) on a voice call: Real-Time Transport Protocol (RTP), RTP Control Protocol (RTCP), or both.

H.323 VoIP Call Preservation Enhancements for WAN Link Failures

Changes made to the Cisco IOS H.323 voice gateway and Cisco Unified CallManager in support of this feature make it possible to preserve calls when the WAN link flaps, resulting in a temporary TCP connection loss between the Cisco Unified CallManager and an IP phone or Cisco IOS H.323 voice gateway located in a remote site or in branch office locations.

Integrated Services

This feature allows data PRI services (dial-in, dial-on-demand routing [DDR], and DDR backup) to occur on top of voice-enabled PRI interfaces. This feature also adds multilevel precedence and preemption (MLPP) capability for DDR calls over the active voice call when no idle channel is available during the DDR call setup.

MLPP is the placement of priority calls through the network. Precedence designates the priority level that is associated with a call. Preemption designates the process of terminating lower-priority calls so that a call of higher precedence can be extended.

With this feature, an ISDN interface can now be configured to accept multiple call types, which will allow integrated data and voice services.

For more information about the Integrated Services feature, see the *Integrating Data and Voice Services for ISDN PRI Interfaces on Multiservice Access Routers* document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xc4/intserv.htm

Video Support for SCCP-Based Endpoints

The Video Support for SCCP-Based Endpoints feature adds video support for Cisco Unified CallManager Express to maintain close feature parity with Cisco Unified CallManager. This feature allows you to use Cisco VT Advantage clients for video calls between SCCP controlled IP Phones or between calls from SCCP controlled IP Phones and H.323 endpoints.

For information about video support in Cisco Unified CallManager Express, see the "Video Support for SCCP-Based Endpoints" chapter in the *Cisco CallManager Express System Administrator Guide* at the following URL:http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_administration_guide_chapter09186a00805f28fb.html

Limitations and Restrictions

There are no known limitations or restrictions.

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 in Cisco IOS Release 12.4(4)T are also in Cisco IOS Release 12.4(11)XJ. For information on caveats in Cisco IOS Release 12.4(4)T, refer to the *Caveats for Cisco IOS Release 12.4(4)T* document. This document lists severity 1 and 2 caveats; the documents are located on Cisco.com and the Documentation CD.

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

This section contains the following caveat information:

Resolved Caveats - Cisco IOS Release 12.4(4)XC7

- 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.

- CSCsd81407

  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

- 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

- 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.

`CSCsg96319 reverse ssh eliminated telnet authention on VTY`

Symptom When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the

ssh -l *userid* **:***number ip-address* command.

Conditions This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804831b6.html

Workaround Configure reverse SSH by entering the **ip ssh port** *portnum* **rotary** *group* command. This configuration is explained at the following URL:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

`CSCsg40567 Memory leak found with malformed tls/ssl packets in http core process`

Symptom Malformed SSL packets may cause a router to leak multiple memory blocks.

Conditions This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

Workaround Disable the **ip http secure server** command.

CSCsg03449 Etherswitch module VLAN Trunking Protocol Vulnerabilities

Symptom

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

Conditions The packets must be received on a trunk enabled port.

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759 -- VTP version field DoS
- CSCse40078/CSCse47765 -- Integer Wrap in VTP revision
- CSCsd34855/CSCei54611 -- Buffer Overflow in VTP VLAN name
- CSCsg03449 -- Etherswitch module VLAN Trunking Protocol Vulnerabilities. Cisco's statement and further information are available on the Cisco public website at: http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

CSCsj44099 Router crashes if DSPFARM profile description is 128 characters long.

Symptom A cisco c3800 router can experience a memory corruption resulting in a crash if the description field under the “dspfarm profile” configuration matches the maximum of 128 characters.

Conditions During configuration of the dspfarm profile thru the CLI, a description that is 128 characters will cause a memory copy problem. If the user tries to display the results of the configuration using “show dspfarm profile”, the router will crash trying to display the output.

Workaround To prevent this problem configure the dspfarm profile description with 127 characters or less.

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

Symptom A router that is running RCP can be reloaded by a specific packet.

Conditions This symptom is seen under the following conditions

  - The router must have RCP enabled.
  - The packet must come from the source address of the designated system configured to send RCP packets to the router.
  - The packet must have a specific data content.

Workaround Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

CSCec12299 Corruption of ext communities when receiving over ipv4 EBGP session

Symptom EIGRP-specific Extended Community 0x8800 is corrupted and shown as 0x0:0:0.

Conditions This symptom is observed when EIGRP-specific Extended Community 0x8800 is received via an IPv4 EBGP session on a CE router. This occurs typically in the following inter-autonomous system scenario:

ASBR/PE-1 <----> VRF-to-VRF <----> ASBR/PE-2

Workaround Use a configuration such as the following to remove extended communities from the CE router:

```
router bgp 1
 address-family ipv4 vrf one
 neighbor 1.0.0.1 remote-as 100
 neighbor 1.0.0.1 activate
 neighbor 1.0.0.1 route-map FILTER in
 exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
 set extcomm-list 100 delete
!
```

CSCse24889 Malformed SSH version 2 packets may cause processor memory depletion

Symptom Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

Conditions This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

Workaround As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t

ip ssh version 1
end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

Workaround

```
10.1.1.0/24 is a trusted network that
```

```
is permitted access to the router, all
other access is denied

access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any

line vty 0 4
access-class 99 in
end
```

Further Problem Description: For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document: http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a0080716ec2.html. For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document: http://www.cisco.com/warp/public/707/ssh.shtml

CSCsc40493 Lengthy PADR frame could crash PPPoE BRAS

Symptom A PPPoE aggregation server (BRAS) may reset when receiving a malformed PPPoE message.

Conditions A malformed PPPoE message must be received on an aggregation interface.

Workaround There is no workaround.

CSCsh53643 mbar/isync compiler automation (No RNE available)

CSCsh77241 Reverting the compiler back to c2.95.3-p11b (No RNE available)

- 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.

Open Caveats - Cisco IOS Release 12.4(4)XC7

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(4)XC6

- CSCsf30058

  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

CSCsb40304

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

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.

`CSCsd92405`

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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

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

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

CSCek48162: TDM cross connects before last call disconnect and assertions

Symptom : Under heavy stress few tdm assertion failures are seen

Conditions :This is seen with SS7 with more than 50 calls per second.

Workaround: There is no workaround

CSCek51075: Assertion failures at **tdm_local_endpoints_connect CSCek61570 Trunk dn** stuck in seize/seize state and does not recover.

Symptom : Few assertions may be seen during bootup and for the first set of calls. This does not have any effect on the system.

Conditions : This may happen in a situation when the calls are cleared as the system goes for a **rommon**.

Workaround : There is no workaround

CSCsb25337:Unnecessary tcp ports opened in default router config Cisco devices running IOS that support voice and are not configured for Session Initiated Protocol (SIP), are vulnerable to a crash. However, these devices are isolated to traffic destined to User Datagram Protocol (UDP) 5060. Devices which are properly configured for SIP processing are not vulnerable to this issue.

Workaround : See the advisory posted at:
http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml

CSCsc72722: CBAC-firewall resets TCP idle timer upon receiving invalid TCP packets

Symptom : TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

Conditions : With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

Workaround : There is no workaround.

CSCsd91454: One way voice traffic due to incorrect **IPHC(UDP) Di0: CS 1 IPCRC**

Symptom : Voice traffic is dropped in one direction due to IPHC IPCRC error.

Conditions :The problem is found some time after the voice call has been established. When the problem is occurring, the logs show IPHC error messages.

Workaround : Use process switching

CSCsd92405: Router crashes on receipt of repeated SSL connection with malformed finished message

Symptom : A router crashes when receiving multiple malformed TLS and/or SSL3 finished messages. A valid user name and password are not required for the crash to occur.

Conditions : This symptom is observed when a router has HTTP secure server enabled and has an open, unprotected HTTP port.

Workaround : There is no workaround, however, user can minimize the chances of the symptom occurring by permitting only legitimate hosts to access HTTP on the router.

CSCse58397: ISDN BRI Dialer Interface is always in up state

Symptom : ISDN B channels are in UP state

Conditions :After reload and after shut/no shut

Workaround : There is no workaround

CSCsf28515: Crashes at mars_default_port_dsp_connect

Symptom : Router crashes at mars_default_port_dsp_connect after call passes through the digital voice-port.

Workaround : There is no workaround

CSCsf28711: 5850 reloads unexpectedly on making a single call CSCsf28840 crash due to configured peer type control vector

Symptom : Active eRSC reloads with traceback when first (PRI/SS7)call is made.

Conditions : This issue is seen when 5850tb is working with 12.4(10.5)PI5 image. Gateway come up with this image, when first (PRI/SS7) call is made the active eRSC reloads unexpectedly with traceback. This reload is seen for both H323 and SIP calls. Similar issue is seen in 5400 when MGCP-SIP call is made.

Workaround :There is no workaround

CSCsg16908: IOS FTP Server Deprecation

CSCsg46546: Erroneous alerting during pickup with CSCek58324. Call focus is wrong after picking up a trunk dn

Symptom : After an attempt to pick up an onhold trunk dn, the call display on the ephone which puts this DN to onhold is messed up. The call can not be picked up successfully by other phone and it becomes the focus one on the phone. The connected trunk dn can not be displayed and other incoming call can not be put on hold.

Conditions : There are two incoming trunk DN calls. The 1st one is answered and then the 2nd one. The 1st one is put onhold automatically when the 2nd one is answered. After the other phone attempts to pick up the 1st call, the pickup fails and the 1st call becomes the focus one on the phone. The softkey is displayed incorrectly.

Workaround : Press the line button to resume the call onhold instead of picking it up from pickup button or fac dialing. However, this workaround can not be applied to a phone which does not have the trunk DN configured.

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 IOS.

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

Workaround : 1) Disable Trans coding (or)

2) Make sure that the Trans coding and Voice Termination are on different DSP(s). This can be performed by configuring the maximum number of trans coding sessions to a value such that it would require a multiple of 240 DSP credits. Example 1:

```
In the following configuration each trans coding session (complexity=high) will require 40
DSP credits. In order to use a multiple of 240 credits, we need to set the maximum trans
coding sessions to 6 (6 * 40 = 240) or any multiple of 6.
dspfarm profile 1 trans code
 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 trans coding sessions to 8 (8 * 30 = 240) or any multiple of 8.


dspfarm profile 2 trans code
 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.

CSCsg59037: 851/871 cannot upgrade rommon from IOS

Symptom : Cisco 851 and 871 routers have no way to remotely upgrade the ROMMON firmware image.

Conditions : Cisco IOS versions for the Cisco 851 and 871 routers did not provide a mechanism to remotely upgrade the ROMMON firmware image.

Workaround : Cisco IOS Release 12.4(11)T1 for the Cisco 851 and 871 router introduces the command upgrade rom-monitor file which allows the ROMMON firmware image to be remotely upgraded. See this link for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tcf_r/cf_13ht.htm#wp1032550

CSCsg66096: Privacy ON: call onhold can be intercepted by directed pickup operation

CSCsg66846: TNP phones opening new call when selecting shared transferring line

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 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 does not 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 a 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 : Setting the transfer system to full blind will prevent the DTMF blocking.

CSCsg70355: New default day light savings summer-time rules from Energy Policy Act of 2005 may cause Cisco IOS to generate timestamps that are off by one hour

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

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

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

CSCsg75035: Async Interface not showing up in the IfIndex from a remote NMS machine

Symptom : The interface is indexed on the router but the snmpwalk/snmpget keywords do not seem to return the value when the **sh snmp mib ifmib ifindex** command is used.

Conditions : This happens when loading a 3825 running **3825-adventerprisek9-mz.124-4.XC5.bin**

Workaround : There is no workaround

Open Caveats - Cisco IOS Release 12.4(4)XC6

There are no known open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(4)XC5

- CSCse56800

  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.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

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

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

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

- CSCsf11855

  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

- CSCse05642

  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

- CSCse68138

  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

CSCek26492

Symptom : A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

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

Conditions : This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

Workaround : Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

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

`CSCsd40334: Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.`

Workaround :Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used. See the advisory posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

`CSCsd58381: Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.`

Workaround :Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used. See the advisory posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

`CSCek56688: Change after-hours login timer to 1 min`

Symptom : The minimum after-hours login timer is 5 minutes. It is too long. Customer wants to be able to deactivate the login in 1 min.

Conditions : The problem is observed when after-hours call blocking is enabled.

Workaround : There is no workaround.

CSCek58324: Call focus is wrong after picking up a trunk dn

Symptom : The call display does not work correctly when attempting to pick up an onhold trunk DN. The call cannot be picked up successfully by any other phone and it becomes the focus one on the single phone. The connected trunk DN cannot be displayed and other incoming calls cannot be put on hold.

Conditions : There are two incoming trunk DN calls. The first one is answered and then the second one. The first one is put onhold automatically when the second one is answered. After the other phone attempts to pick up the first call, the pickup fails and the first call becomes the focus on the single phone. The softkey is displayed incorrectly.

Workaround : Press the line button to resume the call onhold instead of picking it up from pickup button or fac dialing. However, this workaround cannot be applied to a phone that does not have its trunk configured for DN.

CSCsc74157: Pings fails with using ISDN switch-type primary-qsig

Symptom : A ping failed when using ISDN switch-type QSIG.

Conditions : This occurs with a Cisco 3725 and a Cisco 3845 back-to-back with ERNST-T2.

Workaround : There is no workaround.

CSCsd47303: Ephone template for ringing state

Symptom : With Cisco CME 4.0, an ephone-template has states for alerting, seized, connected and idle states. The softkey template needs to be defined for the ringing state (of an incoming call).

Workaround : There is no workaround.

CSCsd48251: Held call on shared line shows From Unknown Number

Symptom : After a certain amount of time, some calls that have been received on a shared line and placed on hold will show From Unknown Number.

Workaround : There is no workaround.

CSCse04642: CME GUI can not change ringtype for sidecar lines when log in as user

Symptom : When you log in as a user in CME GUI, you cannot change the ringtype for sidecar lines. You can change the lines on the ip phone but not the lines that belong to the sidecar. If a user is logged in the Cisco CME GUI (log in as user) and changes the ringtype via GUI for the sidecar line and then hits save, the action will save successfully but when you go to the line again the previous ringtype still shows.

Conditions : The problem is seen on Cisco IOS 12.3(14)T5 Cisco CME 3.3 and ios 12.4(4)XC1 and Cisco CME 4.0.

Workaround : This will work if the user changes from CLI ro log in GUI ad admin.

CSCse05642: I/O memory corruption crash on AS5850

Symptom : A redzone violation causes a Cisco AS5850 to crash.

Conditions : This symptom is observed on a Cisco AS5850 gateway having MGCP-NAS package and outgoing VoIP calls.

Workaround : There is no workaround.

CSCse56800: SIP-3-BADPAIR register timer expiry causes slow memory leak

Symptom : SIP Processes causing slow memory leak when there are no active calls on a Cisco 3725. Specifically, the SIP register timer expiry messages are causing this behavior. Reloading the router does not resolve the issue.

Conditions : The message below is what causes this behavior:

```
007042: Jun 17 15:18:45.024 EDT: %SIP-3-BADPAIR: Unexpected timer 23
(SIP_TIMER_REMOVE_TRANSACTION) in state 27 (SIP_STATE_OPTIONS_WAIT) substate 0
(SUBSTATE_NONE)
```

Workaround : There is no workaround

CSCse68138: Handle fragmented packets in VOIP RTP Lib

Symptom : Router may reload due to fragmented RTP packets. This is a platform independent problem.

Conditions : This problem is likely to happen in networks where VOIP is one of applications and one more segments of network are using low MTU.

Workaround : There is no workaround.

CSCse71162: Change minimum ephone keepalive timer from 10 to 1 second

Symptom : Request to reduce the minimum configurable keepalive timer from 10 to 1 second in CME for SCCP phones.

Workaround : There is no workaround.

CSCse82300: Getting Undefined Tone when we enter a invalid FAC

Symptom : The CFA feature in the Cisco VG224 is enabled and we are dialing an invalid FAC code via callgen. We expect to get a reorder tone immediately but we are getting only the Undefined_tone.

Workaround : There is no workaround.

CSCse83674: FXS port cannot be recovered when offhook with howler tone at end of call

Symptom : Analog FXS port on a Cisco 2800/3800 ISR does not go back to idle if it has been offhook for more than a minute at the end of a call.

Conditions : A and B are two FXS ports on the same router connected to analog phones. A calls B. B answers the call. Once the conversation is done, A hangs up. B does not go onhook. After 60 seconds, B starts hearing offhook alert (howler) tone. Putting B onhook now has no effect. B continues to play offhook alert for the rest of its life until the router is reloaded.

Workaround : There is no workaround.

CSCse87446: Extension assigner defaults provision-tags to 0

Symptom : Extension assigner will chose wrong extension if the provision-tag input is zero.

Workaround : Use the ephone-tag.

CSCsf02737: Memory Corruption Crash at chunk_free_caller

Symptom : A Cisco 3825 running Cisco IOS 12.4-9.T crashed. The decoded tracebacks is as follows:

```
abort
crashdump
chunk_free_caller
free_lite_internal
__free
free
skinny_send_msg_internal
skinny_server_process
r4k_process_dispatch
```

Conditions : This seems similar to CSCsb80447.

Workaround : Configuring **no memory lite** seems to alleviate the crashes.

CSCsf07990: CME Dynamic Hunt-Group Login fails

Symptom : Ephone-1 has extension 88, which is also added as a monitor line on a 7914. The Ephone-2, which is connected to the 7914 is in DND state. Now when you try to login to a hunt-group on ephone-1, it fails because the ephone with the monitor lines is in DND state.

```
Aug 14 08:36:07: SkinnyHGJoinByDn: dn(88), join_code(80), join(1)
Aug 14 08:36:07: Cannot join 88 to hunt group list with dnd on.
Aug 14 08:36:07: ephone-1[13]:SkinnyHGJoinByPhone phone-[7] join 80 failed.
```

Workaround : Ephone with the Cisco IP Phone 7914 should not be in DND state.

CSCsf21007: Ephone hunt-group does NOT present calls to monitored DNs

Symptom : When an ephone hunt-group is configured with **present-call idle-phone**, the ephone hunt-group skips over certain members of the hunt group.

Conditions : The problem is observed when members of the ephone hunt-group are monitored.

Workaround : Do not monitor the members of the hunt-group.

CSCsf21458: SRST Reuses sockets causing phones unregister

Symptom : Registered ephones in SRST mode may unregister and then re register

Conditions : This happens when the phone requests for a socket that has already been used by another ephone.

Workaround : There is no workaround.

CSCsf98754: Inband DTMF should be squelched for calls from POTS to Skinny

Symptom : The following scenario is seen:

```
PSTN === Analog or T1 CAS FXO === CME ------ VG224 ---- Phone or IVR
```

The analog ports on the Cisco VG224 are SCCP controlled by Cisco CME.

For a call between PSTN and a Cisco VG224 port (or an IP Phone), the DTMF detection is turned ON on the FXO port. Along with this, the DSP channel associated with the FXO port is programmed to pass through the DTMF tone in the RTP path instead of suppressing it.

The above manifests into a double DTMF digit scenario and is very well pronounced when the Cisco VG224 port is connected to an IVR system looking for digits. For the endpoints controlled by Cisco CME via SCCP, the DTMF relay happens through out of band SCCP messages. Since the original DTMF digit coming from PSTN is not suppressed, we see two digits reaching the IVR system - one from the SCCP message from Cisco CME to the Cisco VG224 port and the second one embedded in the RTP path.

Conditions : A simple way to reproduce this problem is as follows:

```
Phone----FXS=CME----- IP Phone or VG224
```

Make a call from phone on the left to a CME controlled endpoint. Press a digit button on the left phone and hold it for a long time. The user on the CME controlled endpoint on the right can hear: digit beep, silence and continuous digit beep. If the squelching flag was set on the FXS DSP channel, the user would have heard digit beep, silence and back to voice path.

Workaround : There is no workaround.

CSCsf99737: SRST Locale fail over soft keys still display English

Symptom : SRST fails over from Cisco Unified CallManager still displays English languages in softkey regardless of the languages that is configured in Cisco Unified CallManager.

Workaround : There is no workaround.

Open Caveats - Cisco IOS Release 12.4(4)XC5

There are no known open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(4)XC4

- CSCse68355

  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

CSCsc74783

Symptom : Intrusion Prevention System (IPS) signatures that require inspection of TCP flows below port 550 may not be triggered on a Cisco IOS IPS device.

Conditions : This symptom is observed on a Cisco IOS router that is configured for IPS functionality.

Workaround : Apply CBAC (Context Based Access Control) in addition to IPS.

Further Information: On a Cisco IOS router with IPS (Intrusion Prevention System) enabled, all TCP flows should be subject to TCP stateful inspection until the TCP 3-way handshake is complete. This does not work for TCP sessions with a destination port that is less than 550, if it does not match a predefined signature on the router.

CSCsc74783

Symptom : Intrusion Prevention System (IPS) signatures that require inspection of TCP flows below port 550 may not be triggered on a Cisco IOS IPS device.

Conditions : This symptom is observed on a Cisco IOS router that is configured for IPS functionality.

Workaround : Apply CBAC (Context Based Access Control) in addition to IPS.

Further Information: On a Cisco IOS router with IPS (Intrusion Prevention System) enabled, all TCP flows should be subject to TCP stateful inspection until the TCP 3-way handshake is complete. This does not work for TCP sessions with a destination port that is less than 550, if it does not match a predefined signature on the router.

CSCek47681: Backplane TDM loss and assertion failures

Symptom : Under heavy stress, time division backplane timeslots may be lost over time.

Conditions : The symptom occurs with SS7 and more than 50 calls per second.

Workaround : There is no workaround.

CSCse06975: Traceback at pak_copy_contiguous_to_contiguous when testing multicast

Symptom : The VoIP LMR multicast does not function properly with E&M on the NM-HD-2V network module.

Workaround : There is no workaround.

CSCse16973: **show controller call-counters** displays negative values

Symptom : The **show controller t1 call-counters** command displays negative values for the DSO **Active** counter.

Conditions : The symptom occurs on the Cisco AS5400XM platform for both voice and data calls.

Workaround : There is no workaround.

CSCse18940: Memory depletes when VoAAL2 traffic is passed.

Workaround : There is no workaround.

CSCse27845: One way voice after ringing pickup of transferred at-alert call

Symptom : The called party may not be able to hear the caller.

Conditions : Phones A, B, and C are controlled by the same CME. A calls B. B does an at-alert transfer to C. While C is ringing, B does a ringing pickup on C's extension. One-way voice results with B being unable to hear A.

Workaround : There is no workaround.

CSCse47728: Path confirmation failures are observed with VoATM

Symptom : Path confirmation failures seen with Voice over ATM traffic.

Conditions : This is seen with only with VoAAL2 traffic.

Workaround : There is no workaround.

CSCse50167: Speed dial line buttons disappear from CME phones after the router reloads.

Conditions : The speed dials are configured using an ephone template, which is then applied to the affected phone.

Workaround : Remove and re-apply the ephone template after the router reloads.

CSCse56129: Cisco VG224 erroneously triggers hookflash during CME call pickup interaction

Symptom : On the Cisco VG224, a voice port registered to CallManager Express running. 12.4(4)XC may falsely detect a hookflash in the call pickup case.

Conditions : During call pickup, the CME sends an onhook signal to the VG224 port, presents a new call and immediately instructs the port to move to connected state. During these quick steps, the voice port on the VG224 is erroneously reporting a hookflash.

Workaround : Configure **no supervisory disconnect lcfo** on the Cisco VG224 voice port to avoid the false hookflash detection in the CME call pickup case.

CSCse56660: Inbound calls to fxo port fail (no audio) when caller-id enabled

Symptom : Inbound calls to Foreign Exchange Office (FXO) ports on Cisco IOS VoIP gateways connect, but audio is not present.

Conditions : With caller-id enable configured on FXO ports, the call will connect, but no audio is heard. When this occurs, the following error message can be seen at debug level:

```
Jun 20 01:41:15.855: mbrd_e1t1_vic_connect: setup failed
Jun 20 01:41:15.855: flex_dsprm_tdm_xconn: voice-port(0/0/1), dsp_channel
(/0/2/0)
```

Workaround : Disable caller-id on the voice port.

CSCse59347: CME/SRST IP phone unregister does not down the virtual pots peers

Symptom : Using SRST 4.0 with Cisco Unified CallManager Express, calls may fail with a “user busy” signal.

Conditions : When the IP phone must unregister/fall back to the Cisco Unified CallManager, the virtual POTS dial-peers do not disconnect and calls fail with user busy rather than being sent via the H.323 dial-peer to the Cisco Unified CallManager.

Workaround : There is no workaround.

CSCse69235: 871 XC - S&K interface forwarding results in hung interface

Symptom : VLAN interfaces on Cisco 870 series routers may cease to function under heavy loads.

Conditions : If the 802.1x feature is configured as a layer 3 transport in 12.4(4)XC images and continuous, heavy, and unauthenticated traffic is received on a virtual interface, the router may stop responding.

Workaround : There is no workaround.

CSCse70333: CFwdAll erroneously reconfigured after disabling night service

Symptom : **CFwdAll** incorrectly appears after night service is disabled.

Conditions : **CFwdAll** was initially configured using softkey, and unconfigured through the CLI. On the same DN as CFwdAll was on, night service is enabled and disabled.

Workaround : Remove **CFwdAll** via softkey or reload the router.

CSCsc42589: Reset msg to TAPI client when phone reset restart by CME.

CSCsc72502: The TAPI client may not show the call lines in ringing or connected state for the controlled ephone.

Conditions : If the TAPI client registers to the CME while its controlled ephone has some connected or ringing lines, it would not show their status. It would show them all in IDLE state. This problem occurs in any CME releases.

Workaround : There is no workaround.

CSCse06975: Traceback at pak_copy_contiguous_to_contiguous when testing multicast

Symptom : VoIP LMR multicast capability does not work on network module NM-HD-2V with E&M.

Workaround : There is no work around.

CSCse15025:Intermittent analog/cas voice port lockup or robotic voice

Symptom : An analog or digital CAS port enters a state in which inbound or outbound calls, or both, may no longer function through the port.

Conditions : This symptom is observed on a Cisco 2800 series and Cisco 3800 series that function as gateways with analog or digital CAS ports that use PVDM2 DSP modules.

When this problem occurs, it impacts multiple ports that share the same signaling DSP. The output of the **show voice dsp signaling** EXEC command shows which DSP is used by a port for signaling. The symptom may occur more often for ports that use DSP 1 on the PVDM2 module for signaling.

Because this issue impacts the signaling channels, it has been seen that calls either will not connect at all through impacted ports or in some cases when multiple simultaneous calls are present on adjacent voice ports/timeslots, the call may connect momentarily before being disconnected.

If a problem occurs only on a single voice port, there is another problem, not this caveat (CSCse15025). PRI/BRI calls are not affected because PRI/BRI does not utilize the DSP for signaling purposes.

When the symptom occurs with either a VIC2-xFXO or EVM DID/FXS module, enter the **terminal monitor** command followed by the **test voice port** *port- number* **si-reg-read 39 1** command for one of the affected ports. The output typically should be a single octet value for register 39. When the symptom occurs, information for Registers 40, 41, and 42 is presented and some of the registers show double- octet information. See the example output (2) below.

When the symptom occurs with FXS or analog E&M modules, enter the **terminal monitor** command followed by the **test voice port** *port- number* **codec-debug 10 1** command for one of the affected ports. The output typically should be a single octet value for each register. See the example output (4) below.

Workaround : There is no workaround.

CSCse47338: H245-signal dtmf relay requires signal update to end digits

Symptom : A third party device sends dtmf-relay using a h.245-signal, which includes duration of the digit. The CME gateway sends the digit to CUE, but the digit is not considered done unless another digit is received. This results in %SIP-3-DIGITEND: Missing digit end event messages.

Workaround : Send an extra (unnecessary) digit, which indicates the previous digit is ended.

CSCse60250: Support Localization for the Cisco IP Phone 7906 on Cisco Unified CME.

CSCse66125: Call-waiting ring in ephone-dn-template fails to hold configuration

Symptom : When trying to configure call-waiting ring on an ephone-dn x, the configuration is accepted, but cannot be seen in the configuration.

CSCse75014: CME/SRST not able to make calls to Unity VM

Symptom : With CME/SRST, you are able to make calls to Unity VM.VM port DN is not coming to “Idle” state after restarting Unity.

CSCeh69448: SCCP CME need to clean up tftp binding.

CSCek43094: Add TNP compatible Network locale tags to cnf file.

CSCsc82351:Device ID for the Goped phone is incorrect

Symptom : The device ID for the Goped phone is incorrect.

Workaround : There is no workaround.

CSCsc85575: Subsequent call following a conf call by TNP Ph results in 1-way audio

Symptom : No audio is received from a Cisco 7931 IP phone.

Conditions : This symptom is observed when a call is made between a Cisco IP phone 7960 and a Cisco IP phone 7931. The user of the CiscoIP phone 7960 experiences one-way audio intermittently while the user of the Cisco IP phone 7931 does not experience this symptom.

Workaround : Reset the Cisco IP phone 7931.

CSCsc99639: CME unable to make call on 2nd line using line button when 1 line busy

Symptom : The CME is unable to make call on a second line using line button when line 1is busy

Conditions : This occurs when you make a call from Phone A to Phone B on Line 1. Answer the call on Phone B on line 1. Press Line 2 on Phone B. The first call is put on Hold on Line 1 but Line 2 button light does not come up and Line 2 has no dial tone and it does not accept a new call on Line 2 at all. Ideally Line 2 should put the call on Hold and then accept new call with giving out dial tone.

Workaround : There is no workaround.

CSCsd13066: No caller ID displayed for a forwarded call on IP Phone running 7.x

Symptom : When release 7.x phoneload is used on a forwarding phone, the forward-to party does not see the forwarded party number on the display.

Workaround : There is no workaround.

CSCsd73435: The **button-layout help** CLI is unclear.

CSCsd86966: Not able to create CTL file for 7906 phone.

CSCsd90419: Cisco IP Phone 7941/61/11 does not support localization in SRST

Symptom : The Cisco 7941/61/11 phones display change to English in SRST mode.

Conditions : Phone falls back to SRST CME router.

Workaround : There is now workaround.

CSCse05698: CME 12 build in locales support on 7941/61/11.

CSCse08865: Enhance CME locale installer to support 7941/61/11/70/71

CSCse16210: 7920 locale support enhancement.

CSCse29308: CCME extension assigner extra

CSCse35293: CCME extension assigner need to update CNF file.

CSCse36127: If a Phone is viewed on the GUI the extensions are marked as normal ring even if they are monitored lines. So every time a change is made all lines have to be corrected via the CLI.

Workaround : This defect has been rectified via the CME GUI 4.0.0.1a file package. Download and install this CME GUI file package (or newer) to overcome the problem.

CSCse39419: Some phones XML file does not have correct m_vendor

Symptom : Cannot configure the phone through the vendorConfig in the XML file

Further Problem Description:The VendorConfig is missing in the XML file.

Workaround : There is no workaround.

CSCse41295: MOH debugs flood the console when MOH file is unconfigured

CSCse56023:CME extension assigner clean up

CSCse62649: Change CME GUI logo to Cisco Unified CallManager Express

CSCse65819: Reset needed after extension assignment of 7914 attached phone

Open Caveats - Cisco IOS Release 12.4(4)XC4

There are no known open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(4)XC3

CSCek37177: The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

Symptom This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability. Cisco has made free software available to address this vulnerability for affected customers.

Workaround : There are workarounds available to mitigate the effects of the vulnerability. See the advisory posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml

CSCse37580: Router crashes using the **@ppc_process_dispatch** command.

Symptom : A Cisco router crashes while making a call using the command **test voice port detector ring-trip**.

Workaround : There is no workaround.

CSCse41306: The sound quality of the Music on Hold feed is poor.

Workaround : Using ST-TC1 in tandem with TBB-1 may work in some cases.

CSCse23652: 7912 registered to CME 3.3 running Cisco IOS 12.4(3b) is not able to initiate a call when controlled by the TSP client running TSPv.

Workaround : There is no workaround.

CSCse23304: When selecting "Extensions" in the Configuration drop-down menu in the Call Manager Express GUI for CME 4.0, extension type "Park-Slot" is erroneously listed as being of the type "MWI" and extensions of the type "Paging" are erroneously listed as being of the type "MOH." All other extension types are listed correctly.

Conditions : The symptom occurs on CME 4.0 voice routers using CME GUI version 4.0.0.0.

Workaround Workaround: If CME 4.0 features are not needed, use an earlier release of CME and its corresponding GUI version. If the CME 4.0 features are needed, configure **ephone-dns** and ephones via Cisco IOS CLI.

CSCse20435: Memory runs out and fails the system after extended use.

Conditions : The memory usage increases when an ephone falls back from a CME or CCME to a SRST.

Workaround : There is no workaround.

CSCsd99389: The system reloads when call forwarding is invoked.

Conditions : The symptom occurs if a dialplan pattern and an invalid call forward number are configured.

Workaround : Verify that all call forward numbers are correct or remove the dialplan pattern.

CSCsd57413: Unhide the 7906G-related CLI.

CSCsd46996: A memory leak occurs while upgrading CAPF

Workaround : There is no workaround.

CSCek45370: A dialer interface using VWIC-MFT-2T1/E1 may get an ISDN carrier timeout if the terminating gateway does not have dailer-group configured.

Workaround : Configure dialer-group on the terminating gateway.

CSCek40644: One channel of a DN may get stuck and incoming and outgoing calls cannot be made.

Workaround : Reset the ephone.

CSCsd19564: Button optimization is required for park-recall, pickup-on-hold and pickup-at-alert functions.

CSCsd57096: Configuration is prohibited for certain interfaces through the interface range command.

Conditions : This symptom occurs on all platforms if the interface range command is used to attempt to configure a range of interfaces when the last physical interface in the range itself contains the sub-interfaces.

Workaround : Configure each of the interfaces individually and outside of the interface range command. Another option is to remove the subinterfaces from the last interface in the range prior to attempting the configuration through the range command.

CSCse19112: Caller name does not display on all IP phones that have shared lines or overlay lines.

Workaround : There is not workaround.

CSCse35506: Secondary dialtone is not heard after FAC standard is configured on CME 4.0

Workaround : Call can be placed without the dial tone.

CSCse34614: Caller name does not appear on IP phone display.

Conditions : The symptom occurs with IP phones that are registerd to CME with IOS 12.4(4)XC (CME 4.0), with IP phones that have overlay DNs with call waiting, and with IP phone that has an active call on the overlay dn and a second call is received.

Workaround : There is no workaround.

CSCeg90328: The router crashes when the user tries to convert an sccp phone to an SIP phone.

CSCek34261: A Cisco Integrated SONET/SDH router (ISR) may crash during the "gt96k_mbrd_bri_set_bandwidth" function.

Conditions : This symptom is observed on the Cisco 1800, 2800, and 3800 series routers that function as an ISR when an incoming call is placed with 32KB bandwidth. The symptom does not occur when has a call has 56 KB or 64 KB bandwidth.

Workaround : Deny the invalid incoming call by entering the <CmdBold>isdn caller<noCmdBold> command on the ISR router.

Open Caveats - Cisco IOS Release 12.4(4)XC3

There are no known open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(4)XC2

CSCsd54232: Qsig Call Forward shows AFW memories leak

Symptom : Certain QSIG Call Forward Busy and Call Transfer operations might result in memory leakage.

Workaround : There is no workaround.

CSCsd78806: Can not add ATA through GUI

Symptom : While trying to add an ATA through the GUI for Cisco Unified CallManager Express, e an error is received on the page when you try to save the ATA configuration information and its not possible to add the ATA.

Conditions : This applies to only ATA; when you try to add any other IP phone, the process works fine.

Workaround : Add ATA through the CLI on the router.

CSCsd35389: Deleted ephone-dn's never unregister with Gatekeeper unless GW reloaded

Symptom : Usually CME is automatically registered with a **gatekeeper all** for the ephone-dn, but when a ephone-dn is deleted it never unregisters with the gatekeeper.

Conditions : This problem occurs even if you enter **no gateway** then **gateway** on the CME router to force it to unregister.

Workaround : Reregister the deleted ephone-dn and enter **show back up**.

CSCsd08105: Cisco IP Phone 7960 speaker phone light does not turn off after pressing hold

Symptom : When a call is put on hold on a Cisco IP Phone 7960 and the call is on a speaker phone, resuming on another phone does not clear the speakerphone light (release 7.x phoneload).

Workaround : Depress the speakerphone light to clear it.

CSCsd71081: CME 4 Crashing & Tracebacks when DND button pressed on 7970 with 7914

Symptom : CME 4 Reloads after DND button is pressed.

Conditions : This problem occurs when using the Cisco IP Phone 7970 with the additional 7914 extension module; pressing the DND button causes the CME to produce traceback and reload. This does not occur when the 7914 is not installed.

Workaround : There is no workaround.

CSCsc11833: Intermittent analog or digital CAS port lock up - in/out calls fail

Symptom : An analog or digital CAS port gets into a state where inbound and/or outbound calls through the port may no longer work.

Conditions : This symptom has been seen on Cisco 2800/3800 gateways with analog or digital CAS ports which use PVDM2 DSP modules.

It can take some time for the symptom to occur, but when it does occur, it impacts multiple ports which share the same signaling DSP. To see which DSP a port is using for signaling, check the output of the exec command **show voice dsp signaling**. It has been observed to occur more often with those ports which use DSP 1 on the PVDM2 module for signaling.

If a problem is noticed only on a single voice port, it would not be this issue. Because PRI/BRI does not utilize the DSP for signaling purposes, it is not impacted by this issue.

When the problem occurs and this is either on a VIC2-xFXO or EVM DID/FXS modules, run **test voice port** *port #* **si-reg-read 39 1** on one of the impacted ports. You need to run 'terminal monitor' first to see the output. The output typically should be a single octet value for register 39. When the problem happens, information for Registers 40, 41 and 42 is presented as well and some of the registers show double-octet information.

If using FXS or analog E&M modules, use **test voice port** *port #* **codec-debug 10 1** and compare the output. Again, the normal output will be single octet information for each register. This test only needs to be run on one of the voice ports in this state to confirm if this is the issue being seen.

Workaround : There is no workaround to prevent this problem from occurring. Once in this state, a reload of the gateway is necessary to recover it.

Additional Information: If the problem being seen has been confirmed to be this issue, the software changes associated with this report will mitigate the problem in the majority of cases. It may still be possible to see the problem in some cases and if this is experienced contact Cisco TAC for assistance.

`CSCsd71944: No audio on consult transfer to PSTN with live MOH for local users`

Symptom : This was a bug in the multicast MoH for local SCCP phones features. Multicast MoH was not stopped for the transferee (if it was an SCCP phone) when the transfer was committed.

To check whether you are experiencing this bug, look for debug output similar to the following after the transfer is committed:

```
*Mar 20 23:37:04.795: SkinnyUpdateDnState by EFXS_OPEN_VOICE_PATH
  for DN 1 chan 1 to state CALL_START
*Mar 20 23:37:04.795: ephone-1[3]:UpdateCallState DN 1 chan 1 state 12 calleddn
-1 chan 1
*Mar 20 23:37:04.795: ephone-1[3]:Binding ephone-1 to DN 1 chan 1 s2s:0
*Mar 20 23:37:04.795: SKINNY_CALL_START for DN 1 has call_restart set
*Mar 20 23:37:04.795: SKINNY_CALL_START for DN 1 change to CONNECTED
*Mar 20 23:37:04.795: ephone-1[3]:Call Start ignored - mediaActive set
```

Conditions : The transferee is an SCCP phone listening to multicast MoH supplied by the CME router.

Workaround : A simple workaround is to remove the “multicast moh...” configuration under “telephony-service.”

`CSCsd76246: Intercom not muting 7960s`

Symptom : Cisco IP Phone 7960s are not becoming muting when receiving intercom calls.

Conditions : A Cisco IP Phone 7960 is configured in an intercom dn pair with another phone on the same system.

Workaround : There is no workaround.

CSCsd85687: Secondary number is not considered while parking to reserved-for slot

Workaround : There is no workaround.

CSCsc46528: Sub entry polling: no of rows returned inconsistently from speedbird mib

Symptom : ccmeEphoneActTable from CISCO-CCME-MIB provides inconsistent Vresults.

Conditions : This symptom has been observed when a partial SNMP GET is issued on selected columns from ccmeEphoneActTable.

Workaround : Perform a complete SNMP GET instead of a few entries on ccmeEphoneActTable.

CSCsd91169: Hlog from ringing state allows last agent to logout of b-acd

Workaround : There is no workaround.

CSCsd27683: Cisco IOS gateway does not make H.245 TCP connection after it gets the address

Symptom : A Cisco IOS H.323 gateway (GW) that is running Cisco IOS Release 12.4 (7) is not initiating the H.245 TCP connection.

Conditions : This symptom occurs only if the terminating GW or CCM sends Alert with H.245 Address and PI=1,2,8 in response to a fastStart Setup sent from the originating GW.

Workaround : Perform the following:

- Add **progress_ind alert strip** on outgoing dial peer to TGW in OGW.
- Configure slow start on the gateways. Under voice service VoIP, H.323 mode.

Further Problem Description: An H.323 GW initiates the FS call to another GW or CCM. In response to this, CCM or terminating GW sends slow start Alert with h245 Addr and PI=1,2,8. The phone at the originating GW expects ringing tone from the terminating GW. It is not ringing now, but the phone at the terminating side is ringing. Now if user did not pick the call (i.e. will not send Connect message), then the call will drop. Caller will never come to know what happened at the other end (there is no ringing tone). Without PI in Alert, it works well.

CSCsc94215: Fix indexing in various tables in CISCO-SRST-MIB & related components

Symptom : The index may not come out correctly if doing a get next of an item in a table.

Conditions : This occurs in csrstAliasTable, csrstAccessCodeTable, csrstLimitDNTable, ccmeCorConfTable, ccmeDialplanPatternTable, and csrstSipEndpointTable.

Workaround : Use get bulk to get the complete table, which returns all correct values.

CSCek38822: No-reg doesnt work on SRST

Workaround : There is no workaround.

CSCek40136: The no-reg on ephone-dn should not apply to dialplan-pattern

Symptom : The E164 number cannot be registered if the matched extension in the dialplan-pattern has no-reg configured. The problem started to occur in 12.4(5.11).

Conditions : If the number in the ephone-dn is configured with no-reg, the expanded E164 via dialplan-pattern can't be registered to either Gatekeeper or SIP proxy.

Workaround : The extension needs to be registered in order to have the expanded E164 registered.

CSCsd96951: Call Pickup fails for 2nd channel on dual line ephone dn if 1st is busy

Symptom : Call cannot be picked up on 2nd channel of a dual line ephone-dn.

Conditions : Using CME 4.0 (Cisco IOS Software 12.4.4XC1) and 1st channel of ephone-dn is BUSY.

Workaround : Use a different phone or different ephone-dn (button) on the same phone.

CSCsd9109: Cisco IP Phone 7936 registration blocked by CLI: **no auto-reg-ephone**

Symptom : Cisco IP Phone 7936 will not register with CME:

```
%IPPHONE-6-REG_ALARM:
```

Conditions : This problem occurs in Cisco IOS Software Release 12.4(4)XC. If **no auto-reg-ephone** is configured, then the user is unable to manually register the ephone associated with a Cisco IP Phone 7936.

Open Caveats - Cisco IOS Release 12.4(4)XC2

There are no known open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(4)XC1

CSCed28266: Software forced crash when adding SIP call headers

Symptom : A Cisco gateway may unexpectedly reload because of a software-forced crash when it builds a SIP ACK(nowledgement) or BYE message.

Conditions : This symptom is observed when the gateway receives a SIP response that contains a Record-Route header and a Contact header and when the length of the Contact header exceeds 128*n, in which “n” is the number of URLs in the Record-route header.

Workaround : There is no workaround.

CSCej73716: Dot1x configurations on L2 and L3 ports should be mutually exclusive

CSCek25126: FXO trunk dn and monitoring enhancement for customer

CSCek26750: ogw(h323,slow start)--ipip1(sip)--ipip2(sip)--tgw not working

Symptom : Voice call fails in the following scenario ogw (h323, slow start) -- ipipgw1(sip)---(sip)ipipgw2--tgw(sip)

Conditions : When slow start, delay-media to delay-media being used

Workaround : There is no workaround

CSCek33537: Codec negotiation failed when SIP EP had mix-codec configured

Symptom : SIP EP with different codecs may not able to establish a stable call among them.

Conditions : SIP EP on CME/GW, if different codecs (included using voice-class codec configuration) was set under voice register pool.

Workaround : There is no workaround.

Further Problem Description: A basic call may be established among the SIP EP. But it was not proper setup with correct codec selection. So the subsequent action on the SIP EP, like transfer/forward/conference, etc. may fail.

CSCsb23025: Locale installer does not include CME spec phrases

Symptom : User locale files not available on CME with 7911 phone.

Workaround : Use default locale information.

CSCsb72082: Memory corruption while ending a call

Symptom : A Cisco 3845 acting as a SIP gateway crashes when a call is placed from SIP phone to PBX. PBX is an Avaya s8700.

Conditions : This occurs on a Cisco 3845 running Cisco IOS Release 12.3(11)T9

Workaround : There is no workaround.

CSCsc60509: Memory leak in CCSIP_UDP_SOCKET

Symptom : Low memory condition caused by a leak in CCSIP_SPI_UDP process

Conditions : Memory leak will be seen if there is a re-Subscribe for a call context/out of call context subscription. For gateway this typically will be dtmf subscription.

Workaround : If possible, do not send re-Subscribe/Un-Subscribe.

CSCsd16947: Spurious memory access traceback seen from 7914 button smashing

Symptom : Spurious memory access may be observed on a Cisco Unified CallManager Express under certain conditions when multiple DN buttons configured on an IP phone are pressed repeatedly and randomly.

Conditions : When multiple DN buttons on a phone are pressed randomly and repeatedly.

Workaround : There is no workaround.

CSCsd36869: CME does not put transferred number digits in line focus

Symptom : Status line changes to show from xxxx instead of reading transfer xxxx.

Conditions : This occurs while receiving a call while in the middle of transferring another call on Cisco Unified CallManager Express IP phone.

Workaround : There is no workaround.

CSCsd36943: CME sends incorrect language code to phone

Symptom : Phone in services mode, displays english text when the user-locale is set to Denmark.

Conditions : This occurs when the following output is visible:

```
telephony-service
    user-locale DA
```

Workaround : There is no workaround.

Further Problem Description: If the user-locale of the phone is set to Denmark, the phone sends in “dk” as the accept language in the HTTP headers for IP Phone services. The CCM sends in “da” correctly.

CSCsd39342: Call hung when 487 is not received after Cancel

Symptom : Call legs are hung and memory leak in the stack

Conditions : This issue is seen when a 487 is not received by the SIP gateway after it send out a CANCEL and if the image has the fix for CSCej42804.

Workaround : The remote end must send 487 to the CANCEL.

CSCsd46569: CME delayed call-waiting ring/beep

Symptom : Call-waiting ring or beep does not give initial tone and is delayed 10 seconds.

Conditions : Call-waiting calls on CME. Initially found in Cisco IOS Release 12.4(2)T2 on both firmware 7.2(2) and 7.2(4).

Workaround : There is no workaround.

CSCsd47013: 2nd call callerid not correct with shared lines

Symptom : No call information for the second call is displayed on the shared DN for other phones after the first call is terminated.

Conditions : Two incomings on the same shared DN. After the first call is terminated, the second call should be presented for the shared DN on all phones.

Workaround : There is no workaround.

CSCsd54414: Ringing persists after 1st of 2 shared line calls is answered on another

Symptom : The ephone may continue ringing.

Conditions : If a call of two incoming calls on a shared DN is answered by an ephone, another ephone having this shared DN may continue ringing.

Workaround : Reset the ephone that has this ringing problem.

CSCsd57802: SIP CME: voice register CLI is not available for c2801 adventerprice

Symptom : voice register global command is not accepted.

Conditions : Under **conf t**, voice register command is not an option.

Workaround : There is no workaround.

CSCsd60182: Wrong DN may be chosen for SetCallState on a shared line

Symptom : For the shared DN, the wrong DN may be chosen for the sccp msg of SetCallState.

Conditions : This problem can't be replicated easily. However, it may be observed after several calls to both channels on a shared DN. When the problem occurs, the ephone would not be able to answer a call and may keep ringing. The debug trace would indicate that a DN not configured on the ephone is chosen when sending the call state sccp message to a line.

Workaround : There is no workaround.

CSCsd67460: 7970/71 has erroneous acct, login and flash softkeys

Symptom : On 7970s and 7971s running on CME 4.0, the “Acct”, “Login”, and “Flash” softkeys are wrongly labeled as “No Park”, “Service is”, “CallPark”.

Conditions : Any 7970/7971 firmware.

Workaround : There is no workaround.

CSCek26630: Real call_id to be provided in COT REQ to TSP

Symptom : COT fails for outgoing calls.

Conditions : For the platforms which use TSP for COT processing

Workaround : There is no workaround.

Further Problem Description: Changes made to the platform resulted in this requirement. Unless the real call-id is passed, TSP will not be able to complete the COT and call for outgoing calls. This is because TSP must allocate and use the same DSP for COT and the call for outgoing calls.

See also CSCek34759.

Open Caveats - Cisco IOS Release 12.4(4)XC1

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(4)XC

CSCei33312: Fast dial on ephone-dn does not owrk when ephone trunked to fxo port

Symptom : Outbound calls from ip phone to PSTN using personal speed dial fails when the ip phone is configured to be trunked to an fxo port. It appears that digits are sent before the fxo port is seized completely. Inbound calls from PSTN through fxo port onto ip phone work fine.

Conditions : Condition only occurs when personal speed-dial is used.

Workaround : Do not use trunk configuration

CSCek13657: %SYS-2-NULLCHUNK:Traceback seen at bootup with no startupconfig

Symptom : Traceback Conditions: Bootup

Workaround : There is no workaround.

CSCek25124: Auto-line x answer-incoming enhancement for customer

CSCek25882: Incorrect KS_NO_HLOG4 mask for seized call state

CSCek27807: feature_Vsa not shown in syslog mode

Symptom : The accounting through syslog using gw-accounting syslog does not generate feature-vsa in the output. They are seen on console but not on syslog server.

Conditions : The records are generated for each and every call. The problem is reproduced by making a simple A-B call and collecting the output at syslog server. The gw-accounting syslog needed to be configured globally.

Workaround : There is no workaround.

Further Problem Description: The problem is a Cisco IOS software bug. The generated log did not use the errmsg. Only error messages are sent to syslog.

CSCei77396: enable ip routing causes error msg %FIB-2-IF_NUMBER_ILLEGAL: Attempt

Symptom : FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for Loopback0 with illegal if_number: 0

Conditions : This has been consistently encountered in the case of SSO mode of HA, when the active router which does the switchover comes up again as the standby node.

Workaround : There is no workaround.

CSCek31887: QSIG rose_decode_facilityIE problem

CSCsc42926: One way Video in Skinny-H323 Conferencing

Symptom : Conferencing with CME-Video capable phones results in one-way video, conference initiator's local video screen disappears while remote video screen is still active. The conference participant's local video screen is active while the remote video screen is frozen.

Workaround : There is no workaround.

CSCsc45472: Cleanup of dnagling ccb when back to IDLE

CSCsc46027: 1-way voice for call xfer with xfer party in diff gw

CSCsc48792: spurious access - traceback seen at sstrncpy --> Active_Facility-->AFW

CSCsc48885: spurious access and tracebacks at ConsultRespComplete

CSCsc60999: No Ringback after call is forwaded with CFNA

Symptom : Call originator no longer hear ringback tone after call forward no answer. B has Call Forward No Answer (CFNA) configured. All ports under 12.4(1), 12.4(2), 12.4(3) or 12.4(4) CME control. 1) A calls B. A gets ringback tone 2) B does not answer. After CFNA timeout, call is forward to C 3) C gets ringing tone. But A on longer gets ringback tone.

Conditions : Root Cause seems to be that there is a call flow change on CME side starting 12.4(1): GW receives a stoptone(ringback) after CFNA timeout followed by starttone(ringback) once call is forwarded to C. When GW side gets start tone(ringback tone), it sends ccCallAlert to ccapi->vtsp. But ccAlert is ignored by VTSP due to voice leg is already in alerting state. Thus call originator no longer hears ringback tone.

Workaround : Use CME version XL1 or XL3 which are special CME release version. Send ccGenerateTone(ringback) rather than ccCallAlert when call is in proceeding state and a startTone(ringback) is received from CME/SRST.

CSCsc84018:**bulk-speed-dial** config does not appear under **show telephony-service**

Symptom : The **bulk-speed-dial** configuration command does not appear under telephony-service. Even though there is **show telephony-service bulk-speed-dial** command, it would be good to show the **bulk-speed-dial** in **show telephony-service** or at least in **show telephony-service all**.

Workaround : There is no workaround.

Conditions : This symptom occurs whenever a v-access is cloned from the dialer interface and could be PPPoE, multilink or PPPoA.

Workaround : Configure the **interface mtu** command to the required value.

CSCsd12178: B-ACD: sh ephone-hunt 1 statistics start issue

Symptom : CME with B-ACD: When the show ephone-hunt 1 statistics start fri 8 to fri 17 command is entered, the statistics show from Friday 00:00 to 10:00 AM. The display should show from Friday 8:00 AM to 17:00 PM.

Workaround : There is no workaround.

CSCsd12361: 7960/70/61- Ringer is not stopped after first incoming call is answered

Symptom : The IP phone may conintue ringing after answering an incoming call.

Conditions : If an ephone is running sccp v5 or onwards and there are more than one incoming calls, the phone continues ringing after answering a call by pressing line button or softkey.

Workaround : 1. Running sccp v4 or earlier versions phoneload. 2. Answering a call by lifting the headset or pressing the speakerphone button.

CSCej31527: Qsig BRI ISDN basic call failure

Symptom : Basic Qsig calls via BRI interface fail after new code is collapsed.

Conditions : Basic Call Flows that fail IP-Phone --> CME-----BRI QSIG----PBX--> Phone2

Workaround : There is no workaround.

Open Caveats - Cisco IOS Release 12.4(4)XC

CSCeh35496: **sh isdn active** does not show voice calls for IP Communications Voice/Fax Network Module (back-to-back)

Symptom : The **isdn active** command is not able to display the active/voice call.

Workaround : There is no workaround.

CSCej30662: AudioStream go through CME if Ori EP park the call to 3rd local EP

Symptom : A video call has been established between 2 ip phones. If the originating endpoint parks, then pickup the call, the video is dropped and the call becomes an audio only call.

Workaround : There is no workaround.

CSCek25773: Router crashed when dialer interface come up

Symptom : The Cisco 2811 router crashes when a DDR call is established with certain T1/E1 interfaces.

Conditions : The crashed problem is found if Ernst T interface is also equipped to the gateway.

Workaround : Remove the Ernst T interface from the gateway.

CSCek26954: Qsig: Calling name not shown in called phone at ALERT and CONNECTED

Symptom : When a remote Ephone call is made to an Ephone in PBX CME, the caller name is not displayed on the PBX phone during the ALERT or CONNECTED states.

Workaround : There is no workaround.

CSCek28264: Wrong caller id is wrong when transferring a call out of trunk dn.

Symptom : Caller id update is not supported when a call on a trunk dn is hairpin transferred out to another destination. The destination party continues to see the transferer's party rather then the connected party.

Workaround : There is no workaround.

CSCsc28501: Live only MoH disconnected not fallback to tone-on-hold

Symptom : If only live MoH is configured in CME and the music source is disconnected, user hears dead air.

Conditions : Only MoH live feed is configured, no MoH from flash.

Workaround : Configure MoH from Flash.

CSCsb35485:GUI interface cannot add phone if no auto-reg-ephone

Symptom : CME GUI says “no new phone to add” when trying to add a new phone.

Conditions : **no auto-reg-ephone** is configured under telephony-service.

Workaround : Remove **no auto-reg-ephone telephony-service** (allow auto ephone registration).

CSCsb67970: CME GUI script error

Symptom : The following message is issued when a new phone is added:

```
A script on this page is causing IE to run slowly. If it continues to run, your
computer may become unresponsive. Do you want to continue?
```

Conditions : The problem seems to happen only when there are many Ephones and Ephone-dn in the CME (230 Ephones and 710 Ephone-dn, for instance). The problem stops when the number of Ephones is reduced to 10. If you click on “No” to “Do you want to continue running the script,” the IE freezes for about seven seconds and then you are able to add phones. This seems to happen when CME has a lot of Ephones and/or ephone-dn in the CME.

Workaround : There is no workaround and no functional impact.

CSCsc01531: Router crash when placing more calls than available queue length

Symptom : The router may crash when trying to place more calls in the BACD queue than the configured queue length.

Conditions : This symptom has been observed when more calls are placed to BACD queue than the configured queue length.

Workaround : Set the codec under dialpeer to g711ulaw.

CSCsc04294: BACD AA script crashes on a call after **no moh** and configuring moh again

Symptom : BACD TCL Script may crash and calls drop.

Conditions : This happens when the **no moh** and **moh** commands are entered under telephony-service after BACD has been configured and loaded. **& Live MoH** is not configured.

Workaround : Avoid using the **no moh** and **moh** commands and configure and use Live MoH instead.

CSCsc28450: **show ephone summary** always says MoH Live feed present

Symptom : The **show moh summary** command does not update the MoH live feed status. It always says Live MoH Feed present even when the source is disconnected.

Workaround : To determine if the music signal is too low and not present, find the voice port sourcing the music and enter the **show voice call** *port number* command. Check the input level.

CSCsc56843: CCME display not shown in internationalized language when transferred

Symptom : Ephone 3 calls Ephone 2 and is connected. When you press the transfer button on Ephone 3, the word “transfer” shows in Japanese. When you press the first digit “1” the display is changed to “transfer 1” in English.

Conditions : User-locale is not set to US, United States.

Workaround : There is no workaround.

CSCsc74157: Pings fail with using ISDN switch-type primary-qsig

Symptom : Ping fails intermittently with the isdn primary-qsig switchtype but it works fine with the isdn primary-5ess switchtype.

Conditions : The test has two ernest t2s back-to-back. The test pings the Cisco 3845 serial interface from the Cisco 3725. When the switch-type is set to primary-5ess it always works. When the switch-type is set to primary-qsig, the request fails right away most of the time. Sometimes the first ping works but fails thereafter.

Workaround : There is no workaround.

CSCsc85957: Video is not restored on Hold/Resume with G.729 over H323

Symptom : Video is not restored after resume when the codec is G.729 and the other leg is H323 and Music on Hold is configured.

Workaround : Choose codec G.711u instead of G.729.

CSCsc94466: Traceback at stcapp_handle_call_disconnect_event (dangling ccb present)

CSCsd10942: Stuck button light on 7914 after repeated pressing

CSCsd11395: Pressing in-use shared dn button on 7970 shows wrong line

Symptom : A 7970 phone shares a line with another device. If the other device causes that line to become in-use, and the 7970 user attempts to select that in-use line, the 7970 will open a new call on other lines instead of doing nothing.

Conditions : 7970 and shared lines.

Workaround : There is no workaround.

CSCsd16892: Cisco VG224 power denial click click heard after call park from analog phone

Symptom : Continuos power denial click click is heard under the following condition - analog phone A uner CME control with overlay configured - A calls B and connected - A either blind transfer B to C or park B’s call

Root cause: When A is in pure overlay mode, CME sends onhook to each of the overlay number for A with the same call reference. GW side returns with NewCall for each onhook. This causes confusion on CME side and gets it into infinite loop due to tries to toggle between new call requests.

Workaround : GW side should only response with one new call per call ref. Supression mechanism is now added in GW sw.

CSCsd19496: Missing TsOnHook for ch 2 of hairpin xfer DN has monitor-port-DN LED red

CSCsd35474: Router crashed during the capf upgrade

Symptom : Router crashed when performing the CAPF upgrade

Workaround : There is no workaround.

CSCsc35814: Memory leak with QSIG-rose running Qsig call transfer regression post syn

CSCsd08105:7960 speaker phone light does not turn off after pressing hold

Symptom : When a call is put on hold on a 7960 Cisco IP phone and the call was on speaker phone, resuming on another phone does not clear the speakerphone light (release 7.x phoneload).

Workaround : Depress the speakerphone light to clear it.

CSCsd11990: Dialer does not bind the call in unidirectional ping with specific confg

Symptom : Two routers are connected back-to-back; pings work in one direction but fail in the other direction. The SETUP is received, but the call does not bind and instead gives a dialer error message.

Conditions : In this case, multiple dialer interfaces are configured under same pool. The configuration should have dialer calling numbers to distinguish between the different dialer interfaces in the same pool. In summary, the configuration is not complete to bind the incoming call to a dialer interface.

Workaround : You must configure the **dialer-remote name** with PPP authentication enabled.

CSCsd13066: No caller ID displayed for a forwarded call on IP Phone running 7.x

Symptom : When release 7.x phoneload is used on a forwarding phone, the forward-to party does not see the forwarded party number on the display.

Workaround : There is no workaround.

CSCsd13098: Port monitor ceases to work correctly after re-config of ds0/voice-port

Symptom : When removing and reconfiguring ds0-group that is monitored by a trunk dn port monitor command, the existing trunk monitor logic does not recover the new configuration automatically.

Workaround : Always reconfigure the trunk dn monitor port command after the port that it monitors is reconfigured.

CSCsd19564: Button optimization for park-recall, pickup-on-hold & pickup-at-alert

Symptom : When a trunk dn call that is transferred out of the phone arrives back on a phone that has the shared trunk dn instance, the call is optimized back to that shared trunk dn instance, freeing the transfer-to line button. This operation is done only when the original trunk dn call is transferred. Further work is needed for other operation such as parking the trunk dn call or picking up the call. While the park and pickup operation on a trunk dn call is legal, button optimization is not possible. When the call arrives back on a phone that has the shared trunk dn instance, this call is not optimized back to that trunk dn instance.

Workaround : There is no workaround. The call optimization feature is only possible when the trunk dn call is transferred not when it is parked or picked up.

CSCsd25454: Onhook redial of an fxo trunked dn/line may occasionally fail.

Symptom : Redial while onhook may not always work for a call that needs to be placed over an fxo trunk dn.

Workaround : Offhook redial the call or place the call without redial.

Caveat Updates and Special Notices

The following information has changed since the initial release of this document:

CSCsd28570

Symptom : A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Conditions : Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability. This vulnerability is present in all versions of Cisco IOS that support the **tclsh** command.

Workaround : This advisory with appropriate workarounds is posted at http://www.cisco.com/warp/public/707/cisco-response-20060125-aaatcl.shtml

Further Problem Description: This particular vulnerability only affected Cisco IOS versions 12.3(4)T trains and onwards. (12.3 Mainline is not affected) Please refer to the Advisories "Software Versions and Fixes" table for the first fixed release of Cisco IOS software.

Additional References

Use these release notes with:

- Caveats
- Cross Platform Release Notes for Cisco IOS 12.4T
- Cisco Feature Navigator
- Field Notices
- Bug Toolkit

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

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].

Use this document is to be used in conjunction with the documents listed in the "Additional References" section.