# Release Notes for Cisco AS5350XM and Cisco AS5450XM Universal Gateways for Cisco IOS Release 12.4(4)XC

**June 09, 2008**
**Cisco IOS Release 12.4(4)XC7**
**OL-9581-02 Seventh Release**

**Last Revised: September 24, 2008**

These release notes describe new features and significant software components for the Cisco AS5350XM and Cisco AS5400XM universal gateways 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, changes to the microcode or modem code, and any other important changes. Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.4T* located on Cisco.com.

For a list of the software caveats that apply to Cisco IOS Release 12.4(4)XC4, see the "Caveats" section on page 11 and see the online *Caveats for Cisco IOS Release 12.4T*. The caveats document is updated for every 12.4T maintenance release and is located on Cisco.com.

# Contents

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

# Introduction

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

# System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(4)XC4 and includes the following sections:

- Memory Requirements, page 2
- Supported Hardware, page 3
- Determining the Software Version, page 3
- Upgrading to a New Software Release, page 4
- Feature Set Tables, page 4

## Memory Requirements

Table 1 and Table 2 describe the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 12.4(4)XC on the Cisco AS5350XM and Cisco AS5400XM universal gateways.

***Table 1 Memory Requirements for the Cisco AS5350XM Universal Gateway***

| Feature Set | Software Image | Flash Memory (MB) | DRAM (MB) |
|---|---|---|---|
| IP Plus | c5350-is-mz | 128 | 512 |
| IP Plus IPsec 3DES | c5350-ik9s-mz | 128 | 512 |
| IP Plus IPsec 3DES Lawful Intercept | c5350-ik9su2-mz | 128 | 512 |
| Enterprise Plus | c5350-js-mz | 128 | 512 |
| Enterprise Plus IPsec 3DES | c5350-jk9s-mz | 128 | 512 |

***Table 2 Memory Requirements for the Cisco AS5400XM Universal Gateway***

| Feature Set | Software Image | Flash Memory (MB) | DRAM (MB) |
|---|---|---|---|
| IP Plus | c5400-is-mz | 128 | 512 |
| IP Plus IPsec 3DES | c5400-ik9s-mz | 128 | 512 |
| IP Plus IPsec 3DES Lawful Intercept | c5400-ik9su2-mz | 128 | 512 |
| Enterprise Plus | c5400-js-mz | 128 | 512 |
| Enterprise Plus IPsec 3DES | c5400-jk9s-mz | 128 | 512 |

# Supported Hardware

Cisco IOS Release 12.4(4)XC supports the Cisco AS5350XM and Cisco AS5400XM universal gateways. The supported interfaces and dial feature cards are detailed in Table 3 and Table 4.

*Table 3 Supported Interfaces for the Cisco AS5350XM Universal Gateway*

| Interfaces and Dial Feature Cards | Product Description |
|---|---|
| **Dial Feature Cards** | AS5X-FC |
| | AS535-DFC-60NP |
| | AS535-DFC-108NP |
| | AS535-DFC-CT3 |
| | 2PRI DFC, 4 PRI DFC, 8PRI DFC |
| **LAN Interfaces** | Fast Ethernet 10/100Base-T (RJ-45) |
| **Trunk/Backhaul Interface Options** | CT3 DFC |
| | 2 PRI CT1/CE1 DFC, 4 PRI CT1/CE1 DFC, 8 PRI CT1/CE1 DFC |
| | Two 8-MB serial ports |

*Table 4 Supported Interfaces for the Cisco AS5400XM Universal Gateway*

| Interfaces and Dial Feature Cards | Product Description |
|---|---|
| **Dial Feature Cards** | AS-5X-FC |
| | AS-54-DFC-8CT1/CE1 (8PRI CT1/CE1) |
| | AS54-DFC-CT3 |
| | AS54-DFC-108NP |
| | AS54-DFC-60NP |
| **LAN Interfaces** | Fast Ethernet 10/100BaseT (RJ-45) |
| **Trunk/Backhaul Interface Options** | 8PRI CT1/CE1 DFC |
| | CT3 DFC |

# Determining the Software Version

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

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.4 Software (c5350-is-mz), Version 12.4(4)XC, RELEASE SOFTWARE
```

# Upgrading to a New Software Release

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

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

For Cisco IOS Upgrade Ordering Instructions, see:

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

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

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

http://www.cisco.com/go/cfn

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

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

# Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Cisco IOS Release 12.4(4)XC4 supports the same feature sets as Releases 12.4 and 12.4(4)T. Cisco IOS Release 12.4(4)XC4 is a rebuild of Release 12.4(4)XC and includes only bug fixes, it does not include any new features.

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

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

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

Table 5 lists the new features and feature sets supported by the Cisco AS5350XM and Cisco AS5400XM universal gateways in Cisco IOS Release 12.4(4)XC.

The table uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.

*Table 5 New Feature List for Cisco AS5350XM and Cisco AS5400XM Universal Gateways*

| | **Software Images by Feature Set** | | | | |
|---|---|---|---|---|---|
| **Features** | **IP Plus** | **IP Plus IPsec 3DES** | **IP Plus IPsec 3DES Lawful Intercept** | **Enterprise Plus** | **Enterprise Plus IPsec 3DES** |
| **Voice** | | | | | |
| AMR-NB Codec | Yes | Yes | Yes | Yes | Yes |
| Cisco Unified CME 4.0(4) Extension Assigner | Yes | Yes | Yes | Yes | Yes |
| Modem Relay | Yes | Yes | Yes | Yes | Yes |
| ToIP | Yes | Yes | Yes | Yes | Yes |
| Cisco Fax Relay | Yes | Yes | Yes | Yes | Yes |
| **Other** | | | | | |
| Warm Reload | Yes | Yes | Yes | Yes | Yes |
| Warm Upgrade | Yes | Yes | Yes | Yes | Yes |
| SRTP with H.323 | No | Yes | Yes | No | Yes |
| DSP Voice Quality Statistics | Yes | Yes | Yes | Yes | Yes |
| Fax-Relay Support for SG3 Fax Machines | Yes | Yes | Yes | Yes | Yes |
| H.323 VoIP Call Preservation Enhancements | Yes | Yes | Yes | Yes | Yes |

# New and Changed Information

## New Hardware Features

### New Hardware Features in Cisco IOS Release 12.4(4)XC

The following new hardware feature is supported by the Cisco AS5350XM and Cisco AS5400XM universal gateways for Cisco IOS Release 12.4(4)XC:

#### High-Density Packet Voice Feature Card

The high-density packet voice feature card for Cisco AS5350XM and Cisco AS5400XM universal gateways (product number AS5X-FC) supports up to six high-density packet voice/fax digital signal processor (DSP) modules (product number AS5X-PVDM2-64), providing scalability from 64 to 384 channels. The high-density packet voice feature card for Cisco AS5350XM and Cisco AS5400XM universal gateways with one to six PVDM2-64 modules can be grouped in various combinations to provide the correct number of DSPs depending on the codec type needed and the Cisco AS5350XM or Cisco AS5400XM trunk configuration.

These Cisco AS5X-PVDM2-64 DSP modules feature the latest DSP technology and provide complete flexibility in channel allocation per DSP to achieve highest possible densities.

You can select the minimum number and density-type PVDM2s depending on the voice channels currently needed, and then add more PVDMs as requirements expand. The AS5X-FC supports T1/E1 and CT3 configurations.

The AS5X-FC voice feature card features:

- Port densities on the AS5X-FC voice feature card depend on codec complexity:
  - Low complexity: Up to 384 G.711 ports
  - Medium complexity: Up to 192 G.726, G.729a, G.729ab, Fax Relay ports
  - High complexity: Up to 144 G.729, G.729b, G.723.1, GSMAMR-NB ports (AMR-NB supports a packetization period of 20 ms only)
- Support for packetization periods for all codecs: 10 ms to 30 ms with configurable increments of the minimum defined by the codec or 5 ms, whichever is greater.
- Support for H.323, MGCP, and SIP call control protocols.
- The AS5X-FC voice feature cards are hot-swappable (OIR) and replaceable.
- PVDM2 SIMM is field-replaceable.
- Software-configurable G.168-compliant echo cancellation for tail circuits up to 64 milliseconds.
- VAD, comfort noise generation, adaptive jitter buffering, and caller ID.
- AMR-NB calls are brought up with the common modes from the *mode-set* of both endpoints.

**Note** You must buy a license to access the DSPWare that supports the AMR-NB codec. We recommend that you purchase a Cisco SMARTnet contract in order to streamline the process of getting the AMR-NB codec DSPWare. When obtaining your license, use the following part number:

- FR535XM-AMR-LIC for the Cisco AS5350XM or Cisco AS5400XM.

For more information, contact your Cisco representative or visit the following Cisco.com website to obtain a Cisco SMARTnet contract: http://www.cisco.com/en/US/partner/products/svcs/ps3034/ps2827/ps2978/serv_datasheet09186a0080092491.html

For more information about this feature, see the following URL:

http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2978/serv_group_home.html

# New Software Features

## 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/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps4625/product_data_sheet0900aecd8041c303.html

## New Software Features in Release 12.4(4)XC2

No new software features are in this release.

## New Software Features in Release 12.4(4)XC1

No new software features are in this release.

## New Software Features in Release 12.4(4)XC

The following new software feature is supported by the Cisco AS5350XM and Cisco AS5400XM universal gateways for Cisco IOS Release 12.4(4)XC:

### AMR-NB Codec

Adaptive MultiRate-Narrow Band (AMR-NB) codec is a highly complex multimode codec that supports eight narrow-band speech encoding modes with bit rates between 4.75 and 12.2 kbps. AMR-NB is designed to preserve high speech quality under a wide-range of transmission conditions. Unlike other codecs, AMR-NB readily adapts to different bit rates based on channel conditions during a call.

The AMR-NB codec was originally developed and standardized by the European Telecommunications Standards Institute (ETSI) for Gropue Speciale Mobile (GSM) cellular systems and chosen by the Third Generation Partnership Project (3GPP) as the mandatory codec for third generation (3G) cellular systems.

#### How the AMR-NB Codec Works

The multirate encoding (or multimode) capability of AMR-NB is designed for preserving high speech quality under a wide range of transmission conditions. Unlike other codecs, the AMR-NB codec can adapt to different bit rates (see Table 6 on page 7) based on channel conditions during the call.

*Table 6 AMR Codec Modes and Bit Rates*

| Codec Mode | Bit Rate (kbps) |
|---|---|
| 0 | 4.75 |
| 1 | 5.15 |
| 2 | 5.90 |
| 3 | 6.70 |
| 4 | 7.40 |
| 5 | 7.95 |
| 6 | 10.2 |
| 7 | 12.2 |
| 8[1] | 1.80 |

[1] Used for Silence Indication Detection(SID) frames.

To perform mode adaptation, the decoder (speech receiver) sends a signal to the encoder (speech sender) to indicate which new mode it prefers. This mode-change signal is called codec mode request (CMR). Because speech is sent in both directions between the two ends in most sessions, the mode requests from the decoder at one end to the encoder at the other end are sent in a piggyback form over the speech frames in the reverse direction; there is no out-of-band signaling needed for sending CMRs. The Cisco AS5350XM and Cisco AS5400XM cannot initiate CMRs, but received CMRs can be processed. For more information about AMR-NB codecs, see RFC 3267.

For more information on this feature, see the following URL:

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

### H.323 VoIP Call Preservation Enhancements for WAN Link Failures

H.323 VoIP call preservation enhancements for WAN link failures sustain connectivity for H.323 topologies where signaling is handled by an entity that is different from the other endpoint, such as a gatekeeper that provides routed signaling or a call agent, such as the Cisco BTS 10200 Softswitch, Cisco PGW 2200, or Cisco Unified CallManager, that brokers signaling between the two connected parties.

Call preservation is useful when a gateway and the other endpoint (typically a Cisco Unified IP phone) are collocated at the same site and the call agent is remote and therefore more likely to experience connectivity failures.

Configuration information for the H.323 VoIP Call Preservation Enhancements for WAN Link Failures feature is included in the “Configuring H.323 Gateways” chapter in the *Cisco IOS H.323 Configuration Guide*, Release 12.4T at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/srst/srst40/srst40ad/srs_call.htm#wp1014888

## Software Features Ported from Other Platforms in Release 12.4(4)XC

The following features have been previously released on other Cisco access servers and high availability platforms. Therefore the individual platform name may not be referenced for the universal gateways. Other differences may exist for the various platforms that are documented.

**Note** The features listed in this section are available only when using the AS5X-FC voice feature card.

### Modem Relay

Modem relay demodulates a modem signal at one voice gateway and passes it as packet data to another voice gateway where the signal is remodulated and sent to a receiving modem. On detection of the modem answer tone, the gateways switch into modem passthrough mode and then, if the call menu (CM) signal is detected, the two gateways switch into modem relay mode.

For more information about this feature, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/mdmrly.html

### Text over IP

Cisco Text Relay implements a mechanism for transporting Text Telephone (TTY) signals over Voice over IP (VoIP) calls in a highly reliable way. Cisco Text Relay transports both TTY text characters and voice over the same channel, supporting both Voice Carry Over (VCC) and Hearing Carry Over (HCO).

Cisco Text Relay is gateway controlled, enabling it to work independently from the call agent. It can be configured on supported gateways for the SIP, H.323, and MGCP.

### Cisco Fax Relay

Cisco fax relay is the default mode for passing faxes through a VoIP network, and Cisco fax relay is the default fax relay type on Cisco voice gateways. Cisco fax relay uses Real-Time Transport Protocol (RTP) to transport the fax data.

For more information about this feature, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_fax_services_over_ip_application_guide/cisrly.html

### Warm Reload

The warm reload feature allows users to reload without reading images from storage. That is, the Cisco IOS image reboots without ROM monitor mode (ROMMON) intervention by restoring the read-write data from a previously saved copy in the RAM and by starting execution without either copying the image from flash to RAM or self-decompression of the image. Thus, the overall availability of your system improves because the time to reboot is significantly reduced.

For more information about this feature, see the following URL:

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/warm_reload_ps6441_TSD_Products_Configuration_Guide_Chapter.htmll

### Warm Upgrade

The warm upgrade feature provides the capability for a Cisco IOS image to read and decompress another Cisco IOS image and then transfer control to this new image. This functionality reduces the downtime of a device during planned Cisco IOS software upgrades or downgrades.

For more information about this feature, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hcf_c/ch40/hwarmup.htm#wp1027129

### SRTP with H.323

Secure Real-Time Transport (SRTP) mode provides secure Voice over IP (VoIP) calls by addressing security requirements for privacy, integrity, and confidentiality of voice conversations. IPsec, a standards-based set of security protocols and algorithms, ensures that signaling information that is sent between the gateway and Cisco Unified CallManager are encrypted. Media encryption using standards-based SRTP ensures that media streams between supported devices are secure.

For more information about this feature, see the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/feature/module/9.8_1_/SRTP.html

### DSP Voice Quality Statistics

The Cisco AS5350XM and Cisco AS5400XM universal gateways support the Digital Signal Processor (DSP) voice quality statistics in Media Gateway Control Protocol (MGCP) calls using Delete Connection (DLCX) messages.

For more information about this feature, see the following URL:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtdspsts.html

### Fax-Relay Support for SG3 Fax Machines

This feature allows Super Group 3 (SG3) fax machines to interoperate over T.38 fax-relay or Cisco fax-relay networks. The capability to interoperate over fax-relay networks is achieved by enabling SG3 fax machines to negotiate down to G3 speeds by suppressing the SG3 V.8 fax call menu (CM) signal. The suppression of the SG3 V.8 fax CM signal (or message) is also known as SG3 spoofing.

For more information about this feature, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/sg3spoof.html

# MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://www.cisco.com/go/mibs

# Limitations and Restrictions

- Before you can run the high-density packet voice feature card for the Cisco AS5350XM or Cisco AS5400XM universal gateway, you must install an IP Plus image (minimum) of Cisco IOS Release 12.4(4)XC or a later release.
- Software echo cancellation is the default configuration—G.168-compliant echo cancellation is enabled by default with a coverage of 64 milliseconds. Hardware echo cancellation is not available.
- Only Packet Fax/Voice DSP modules (PVDM2s) are supported on the Voice Feature Card.
- GSMAMR NB codec support is available only with H.323 and Session Initiation Protocol (SIP) as call control protocols.
- Skinny Client Control Protocol (SCCP) is not supported.
- To use the AS5X-FC voice feature card in your gateway, at least one card must be present during bootup. Additional AS5X-FC voice feature cards can be installed later.
- If you use AMR-NB DSPware, all the DSPs in the system must be upgraded with the GSM AMR-NB supported DSPware.
- A mix of ASFX-FC voice feature cards and NextPort dial feature cards (NP DFCs) is not supported. If the AS5X-FC voice feature card is installed in a Cisco AS5350XM universal gateway with an NP
- DFC running, you must reboot the system to support the ASFX-FC voice feature card, and the NP DFC will be powered down. That is, if the AS5X-FC card is present during bootup, dial-only and universal port cards will not be operational.

**Note** If no AS5X-FC voice feature card is installed during bootup, the gateway will support only dial-only or universal port cards. To use the AS5X-FC voice feature card, you must install the card and reboot the system.

- The following message displays when an upgrade takes place if a version of DSPWare other than the recommended version is uploaded:

```
WARNING: Recommended GSM AMR-NB supported DSPWare for this Cisco IOS image is X.Y.Z
Where X.Y.Z changes depending on the Cisco IOS image that is used by the customer.
```

This warning has no impact on the firmware upgrade and calls can be brought up with a version of DSPWare that is not the recommended version.

## Deferrals

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

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

## Field Notices and Bulletins

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

http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/1654_pp.html

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

# Caveats

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

Caveats in Release 12.4T are also in Release 12.4(4)XC4. For information on caveats in Cisco IOS Release 12.4T, see the *Caveats for Cisco IOS Release 12.4T* document. This document lists severity 1 and 2 caveats; the documents are located on Cisco.com.

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

## 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 authentication 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/docs/ios/12_3t/12_3t11/feature/guide/gt_rssh.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 through 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.

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.

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/docs/ios/security/configuration/guide/sec_cntrl_acc_vtl.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)

## 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 Cisco IOS software.

**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)XC5

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.shtml

`CSCsd40334 Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software.`

**Conditions** 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** There are workarounds available to mitigate the effects of the vulnerability. Cisco has made free software available to address this vulnerability for affected customers.The workaround depends on the condition whether Mobile IPv6 is used and, what version of 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.`

**Conditions** 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** There are workarounds available to mitigate the effects of the vulnerability. Cisco has made free software available to address this vulnerability for affected customers. The workaround depends on whether 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 Unified CallManager Express 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 Unified CallManager Express 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 Unified CallManager Express 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 Release12.3(14)T5 Cisco Unified CallManager Express 3.3 and ios 12.4(4)XC1 and Cisco CME 4.0.

**Workaround** This will work if the user changes from CLI or 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.

`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
```

```
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.
```

**Conditions** This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

**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. See the advisory posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml.

## Open Caveats - Cisco IOS Release 12.4(4)XC3

There are no known open caveats in this release.

## Resolved Caveats - Release 12.4(4)XC2

```
CSCek30937 5400 crash after 30hrs with 644 SRTP calls
```

**Symptom** The AS5400XM system reloads when it handles SRTP traffic with large number of calls.

**Conditions** This problem is caused when the system is under heavy load conditions, and it’s only observed on an AS5400XM when handling SRTP traffic.

**Workaround** Do not make large number of calls or do not configure for SRTP.

```
CSCsd73850 Path confirmation failure for MGCP calls with G726r16
```

**Symptom** Path confirmation failed for MGCP calls with G726r16 codec.

**Conditions** When the calls are made between NP108 and the AS5X-FC voice feature card

**Workaround** Configure **mgcp rtp payload-type g726r16 static** at both gateways.

## Open Caveats - Release 12.4(4)XC1

```
CSCsd71195 Path confirmation failed for MGCP calls, NP108
```

**Symptom** Path confirmation failed for MGCP calls

**Conditions** Symptom occurs when calls are made between NP108 and AS5X-FC voice feature card.

**Workaround** Configure the command **no voice-fastpath enable**.

```
CSCsd73850 Path confirmation failure for MGCP calls with G726r16
```

**Symptom** Path confirmation failed for MGCP calls with G726r16 codec.

**Conditions** Symptom occurs when calls are made between NP108 and AS5X-FC voice feature card.

**Workaround** Configure the command **mgcp rtp payload-type g726r16 static** at both the gateways.

## Open Caveats - Release 12.4(4)XC

```
CSCsd28570 tclsh bypass of AAA authorization commands
```

**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 the following URL: 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.

```
CSCek32317 Dangling session and channel blocked after SS7 NI2 COT voice stress test
```

**Symptom** The SS7 cot function is not working with the AS5X-FC voice feature card.

**Workaround** There is no workaround.

# Additional References

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents, page 42
- Platform-Specific Documents, page 43

## Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Cisco IOS Release 12.4(4)XC4. They are located on Cisco.com:

- *Cross-Platform Release Notes for Cisco IOS Release 12.4(4)T*
- *Caveats for Cisco IOS Release 12.4* and *Caveats for Cisco IOS Release 12.4T*

## Platform-Specific Documents

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

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

## Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.4 and 12.4(4)XC4, and are updates to the Cisco IOS documentation set. Module consists of a brief overview of the feature and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next release of the Cisco IOS documentation set.

## Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Cisco Feature Navigator is available 24 hours a day, 7 days a week.

To use Cisco Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Cisco Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Cisco Feature Navigator at the following URL:

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

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form.

### Documentation Modules

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

### Release 12.4 Documentation Set

Table 7 describes the contents of the Cisco IOS Release 12.4 software documentation set, which is available in both electronic and printed form.

**Note** You can find the most current Cisco IOS documentation on Cisco.com in pdf or html form.

**Note** Some aspects of the complete Cisco IOS Release 12.4 software documentation set might not apply to the Cisco AS5350XM universal gateway.

*Table 7 Cisco IOS Release 12.4 Documentation Set*

| Books | Major Topics |
|---|---|
| • *Cisco IOS Configuration Fundamentals Configuration Guide*<br>• *Cisco IOS Configuration Fundamentals Command Reference* | Cisco IOS User Interfaces<br>File Management<br>System Management |
| • *Cisco IOS Bridging and IBM Networking Configuration Guide*<br>• *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2*<br>• *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2* | Transparent Bridging<br>SRB<br>Token Ring Inter-Switch Link<br>Token Ring Route Switch Module<br>RSRB<br>DLSW+<br>Serial Tunnel and Block Serial Tunnel<br>LLC2 and SDLC<br>IBM Network Media Translation<br>SNA Frame Relay Access<br>NCIA Client/Server<br>Airline Product Set<br>DSPU and SNA Service Point<br>SNA Switching Services<br>Cisco Transaction Connection<br>Cisco Mainframe Channel Connection<br>CLAW and TCP/IP Offload<br>CSNA, CMPC, and CMPC+<br>TN3270 Server |
| • *Cisco IOS Dial Technologies Configuration Guide: Dial Access*<br>• *Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications*<br>• *Cisco IOS Dial Technologies Command Reference, Volume 1 of 2*<br>• *Cisco IOS Dial Technologies Command Reference, Volume 2 of 2* | Dial Access<br>Modem and Dial Shelf Configuration and Management<br>ISDN Configuration<br>Signaling Configuration<br>Point-to-Point Protocols<br>Dial-on-Demand Routing<br>Dial Backup<br>Dial Related Addressing Service<br>Network Access Solutions<br>Large-Scale Dial Solutions<br>Cost-Control Solutions<br>Internetworking Dial Access Scenarios |
| • *Cisco IOS Interface Configuration Guide*<br>• *Cisco IOS Interface Command Reference* | LAN Interfaces<br>Serial Interfaces<br>Logical Interfaces |
| • *Cisco IOS IP Configuration Guide*<br>• *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*<br>• *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*<br>• *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast* | IP Addressing<br>IP Services<br>IP Routing Protocols<br>IP Multicast |
| • *Cisco IOS AppleTalk and Novell IPX Configuration Guide*<br>• *Cisco IOS AppleTalk and Novell IPX Command Reference* | AppleTalk<br>Novell IPX |

*Table 7 Cisco IOS Release 12.4 Documentation Set (continued)*

| Books | Major Topics |
|---|---|
| • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide*<br>• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference* | Apollo Domain<br>Banyan VINES<br>DECnet<br>ISO CLNS<br>XNS |
| • *Cisco IOS Voice, Video, and Fax Configuration Guide*<br>• *Cisco IOS Voice, Video, and Fax Command Reference* | Voice over IP<br>Call Control Signaling<br>Voice over Frame Relay<br>Voice over ATM<br>Telephony Applications<br>Trunk Management<br>Fax, Video, and Modem Support |
| • *Cisco IOS Quality of Service Solutions Configuration Guide*<br>• *Cisco IOS Quality of Service Solutions Command Reference* | Packet Classification<br>Congestion Management<br>Congestion Avoidance<br>Policing and Shaping<br>Signaling<br>Link Efficiency Mechanisms |
| • *Cisco IOS Security Configuration Guide*<br>• *Cisco IOS Security Command Reference* | AAA Security Services<br>Security Server Protocols<br>Traffic Filtering and Firewalls<br>IP Security and Encryption<br>Passwords and Privileges<br>Neighbor Router Authentication<br>IP Security Options<br>Supported AV Pairs |
| • *Cisco IOS Switching Services Configuration Guide*<br>• *Cisco IOS Switching Services Command Reference* | Cisco IOS Switching Paths<br>NetFlow Switching<br>Multiprotocol Label Switching<br>Multilayer Switching<br>Multicast Distributed Switching<br>Virtual LANs<br>LAN Emulation |
| • *Cisco IOS Wide-Area Networking Configuration Guide*<br>• *Cisco IOS Wide-Area Networking Command Reference* | ATM<br>Frame Relay<br>SMDS<br>X.25 and LAPB |
| • *Cisco IOS Mobile Wireless Configuration Guide*<br>• *Cisco IOS Mobile Wireless Command Reference* | General Packet Radio Service |

*Table 7 Cisco IOS Release 12.4 Documentation Set (continued)*

| Books | Major Topics |
|---|---|
| - *Cisco IOS Terminal Services Configuration Guide*<br>- *Cisco IOS Terminal Services Command Reference* | ARA<br>LAT<br>NASI<br>Telnet<br>TN3270<br>XRemote<br>X.28 PAD<br>Protocol Translation |
| - *Cisco IOS Configuration Guide Master Index*<br>- *Cisco IOS Command Reference Master Index*<br>- *Cisco IOS Debug Command Reference*<br>- *Cisco IOS Software System Error Messages*<br>- *New Features in 12.4-Based Limited Lifetime Releases*<br>- *New Features in Release 12.4T*<br>- *Release Notes (Release note and caveat documentation for 12.4-based releases and various platforms)* | |

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, 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:

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:

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

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

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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.