Release Notes for Cisco 1800 Series Routers with Cisco IOS Release 12.4(11)XJ

March 26, 2008
Cisco IOS Release 12.4(11)XJ6
OL-12253-03 Fifth Release
Last Updated: September 24, 2008

These release notes describe new features and significant software components for the Cisco 1800 series routers that support Cisco IOS Release 12.4(11)XJ. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* located on Cisco.com.

For a list of the software caveats that apply to the Release 12.4(11)XJ releases**,** see the "Caveats" section on page 10, and see the online *Caveats for Cisco IOS Release 12.4(4)T* document. The caveats document is updated for every 12.4T maintenance release and is located on Cisco.com.

We recommend 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/cfn.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/cfn.html.

Contents

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

System Requirements

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

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

Memory Requirements

Table 1 lists the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 12.4(11)XJ on the Cisco 1800 series routers.

Table 1 Memory Requirements for the Cisco 1800 Series Routers

Platform	Image Name	Image	Flash (MB)	Ram (MB)
Cisco 1801, Cisco 1802, Cisco 1803	IP Broadband	c180x-broadband-mz	32	128
	Advanced IP Services	c180x-advipservicesk9-mz	32	128
	Advanced Enterprise Services	c180x-adventerprisek9-mz	32	128
Cisco 1811, Cisco 1812	Advanced IP Services	c181x-advipservicesk9-mz	32	128
	Advanced Enterprise Services	c181x-adventerprisek9-mz	32	128
Cisco 1841	Cisco 1841 IOS Advanced IP Services Cisco 1841 IOS ASK9-AISK9 Feature Set Factory UPG For Bundles Cisco 1841 IOS BB-AISK9 Feature Set Factory UPG For Bundles Cisco 1841 IOS AISK9-AISK9 Feature Set Factory UPG For Bundles	c1841-advipservicesk9-mz	64	192

Platform	Image Name	Image	Flash (MB)	Ram (MB)
Cisco 1841	Cisco 1841 IOS Advanced Enterprise Services Cisco 1841 IOS AISK9-AESK9 Feature Set Factory Upgrade For Bundles Cisco 1841 IOS ASK9-AESK9 Feature Set Factory UPG For Bundles Cisco 1841 IOS BB-AESK9 Feature Set Factory UPG For Bundles	c1841-adventerprisek9-mz	64	192
	Cisco 1841 IOS Advanced Security Cisco 1841 IOS BB-ASK9 Feature Set Factory UPG For Bundles Cisco 1841 IOS ASK9-ASK9 Feature Set Factory UPG For Bundles	c1841-advsecurityk9-mz	64	192
	Cisco 1841 IOS Broadband Cisco 1841 IOS BB-BE Feature Set Factory Upgrade For Bundles	c1841-broadband-mz	32	128
	Cisco 1841 IOS Enterprise Base w/o Crypto	c1841-entbase-mz	64	128
	Cisco 1841 IOS Enterprise Base	c1841-entbasek9-mz	64	128
	Cisco 1841 IOS Enterprise Services w/o Crypto	c1841-entservices-mz	64	192
	Cisco 1841 IOS Enterprise Services	c1841-entservicesk9-mz	64	192
	Cisco 1841 IOS IP Base w/o Crypto	c1841-ipbase-mz	32	128
	Cisco 1841 IOS IP BASE	c1841-ipbasek9-mz	32	128
	Cisco 1841 IOS SP SERVICES Cisco 1841 IOS BB-SPSK9 Feature Set Factory Upgrade For Bundles Cisco 1841 IOS SPSK9-SPSK9 Feature Set Factory Upgrade For Bundles	c1841-spservicesk9-mz	64	128

Hardware Supported

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

- Cisco 1801
- Cisco 1802
- Cisco 1803
- Cisco 1811
- Cisco 1812
- Cisco 1841

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 6. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1800 series routers, which are available on Cisco.com at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1800fix/index.htm

Determining the Software Version

To determine which version of the Cisco IOS software is currently running on your Cisco 1800 series (fixed) routers, log in to the router, and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number on the second output line.

```
Router>show version
Cisco IOS Software, C1800 Software (C1800-ADVENTERPRISEK9-M), Version 12.4(11)XJ, EARLY
DEPLOYMENT RELEASE SOFTWARE
Copyright (c) 1986-2006 by Cisco Systems, Inc
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see the *Software Installation and Upgrade Procedures*, which are located on Cisco.com.

Feature Set Tables

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. 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 U.S. government regulations. When applicable, the purchaser/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.

The feature set tables have been removed from the Cisco IOS Release 12.4 release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS 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

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

http://www.cisco.com/support/FeatureNav/FNFAQ.html

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.4 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Search by feature**.

Step 2 To find a feature, use either “Search by full or partial feature name” or “Browse features in alphabetical order.” Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the Features available text box on the left side of the web page.

Step 3 Select a feature from the Features available text box, and click the **Add** button to add a feature to the Features selected text box on the right side of the web page.

Note To learn more about a feature in the list, click the Show Description(s) button below the Features available text box.

Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.

Step 4 Click **Continue** when you are finished selecting features.

Step 5 From the Major Release drop-down menu, choose **12.4**.

Step 6 From the Release drop-down menu, choose the appropriate maintenance release.

Step 7 From the Platform drop-down menu, select the appropriate hardware platform. The “Search Results” table will list all the software images (feature sets) that support the feature(s) that you selected.

Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.4, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Compare Images**, and then **Search by Release**.

Step 2 In the “Find the features in a specific Cisco IOS release, using one of the following methods:” area, choose **12.4** from the Cisco IOS Major Release drop-down menu.

Step 3 Click **Continue**.

Step 4 From the Release drop-down menu, choose the appropriate maintenance release.

Step 5 From the Platform drop-down menu, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down menu, choose the appropriate feature set. The “Search Results” table will list all the features that are supported by the feature set (software image) that you selected.

Table 2 lists the features and feature sets that are supported in Cisco IOS Cisco IOS Release 12.4(11)XJ.

The table uses the following conventions:

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

Note These feature set tables contain only a selected list of features, which are cumulative for Release 12.4(4)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in the *Cross-Platform Release Notes for Cisco IOS Release 12.4(11)T* and Release 12.4(4)T Cisco IOS documentation.

Table 2 Feature List for Cisco 1800 Series Routers

Feature	In	Image
USB eToken 64KB smartcard support	12.4(11)XJ	All. See Table 1 for images
USB Boot Feature		
ADSL2/2+ Annex M Support		
HWIC-4SHDSL and HWIC-2SHDSL Support		
HWIC and VLAN Feature Enhancements		
Wireless LAN Features		

New and Changed Information

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

There are no new hardware features in this release.

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

There are no new software features in this release.

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

There are no new hardware features in this release.

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

There are no new software features in this release.

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

There are no new hardware features in this release.

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

The following new software features are supported in this release.

- USB eToken 64KB smartcard support, page 7
- USB Boot Feature, page 8

USB eToken 64KB smartcard support

The Cisco universal serial bus (USB) eToken 64KB smartcard support feature enables device authentication and simplifies the deployment and secure configuration of Cisco routers. It uses smart card technology in a USB form factor to facilitate the authentication and configuration process. The token provides secure access to the route. The token and a PIN are necessary to access the configuration, keys, and credentials.

Some Cisco access router models have USB ports that can be used with Cisco USB flash memory modules or with the Aladdin USB eToken Pro key. These USB modules can be used with a supported Cisco access router for the following functions:

- USB eToken Pro key provides a secure means of storing and deploying information, such as a bootstrap configuration or VPN credentials, apart from the router chassis. The USB eToken uses smart card technology to protect a small area of memory.
- The USB eToken grants access using a personal identification number (PIN). When IP Security (IPSec) VPN credentials are stored on the USB eToken, they are outside the router. When the USB eToken is inserted in a USB port, and when the user enters the PIN and unlocks the USB eToken,

the user retrieves the credentials and copies them into running memory. When the USB eToken is removed, the router erases the credentials from running memory, ensuring that they cannot be retrieved from the router itself.

USB Boot Feature

The USB Boot feature supports booting from ROMMON and IOS. Platforms can boot from USB in ROM monitor with or without a compact flash device. It is not necessary to use a bootloader image from the compact flash device. Partitions, such as usbflash0:2:image_name, are not supported on USB flash drives.

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

The following new hardware feature is supported in this release:

- HWIC and VLAN Feature Enhancements, page 8

HWIC and VLAN Feature Enhancements

The Cisco Fast Ethernet HWICs are single-wide interface cards, available as a 1-port HWIC (HWIC-1FE) and as a 2-port HWIC (HWIC-2FE), that provide Cisco modular and integrated services routers with additional line-rate Layer 3 routed ports. The following enhancements have been made in Cisco IOS Release 12.4(11)XJ:

- Extended VLAN ID
- HWIC-1FE Routed Port
- HWIC one FE and two FE ports

For more information about these features, see the following documentation on Cisco.com:

- *Cisco Interface Cards Hardware Installation Guide*
- *Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information*

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

The following new software features are supported in this release:

- ADSL2/2+ Annex M Support, page 8
- HWIC-4SHDSL and HWIC-2SHDSL Support, page 9
- Wireless LAN Features, page 9

ADSL2/2+ Annex M Support

The asymmetric digital subscriber line (ADSL) 2/2+ Annex M feature supports routed bridge encapsulation over VC bundles on specific platforms in Cisco IOS Release 12.4(11)XJ. (ADSL) 2/2+ Annex M supports an upstream data rate of up to 3 Mbps and a downstream data rate of up to 24 Mbps. The increase of the Annex M (upstream) data rate is achieved by using some of the tones that were previously used in the downstream data rate in Annex A. As a result, downstream data rates are decreased in Annex M.

The ADSL training log generation command, **dsl-enable-training-log**, has been enhanced to specify the time when to capture a log file. This enables the training log to record firmware debug messages.

HWIC-4SHDSL and HWIC-2SHDSL Support

The G.SHDSL HWICs support up to four pairs of digital subscriber lines (DSL): two inverse multiplexing over ATM (IMA) lines, and two ATM segmentation and reassembly (SAR) lines. The four DSL pairs are bundled in groups and configured in the Cisco IOS command-line interface (CLI) by using the **dsl-group** command.

- The HWIC-2SHDSL provides two ports of connectivity through one *RJ-11* connector. It supports *1-Pair* groups or *2-Pair* groups.
- The HWIC-4SHDSL provides four ports of connectivity through one *RJ-45* connector. It combines four ports of data into one line or two lines with either inverse multiplexing over ATM (*IMA*) groups or *M-pair* groups, and it supports *1-Pair* groups or *2-Pair* groups.

Wireless LAN Features

The following features are supported on the wireless LAN (WLAN).

Access Point Link Role Flexibility

Access Point Link Role Flexibility allows access point radios to operate in a combination of radio roles, such as access point root, bridge root (with or without clients), bridge nonroot (with or without clients). This provides a more flexible deployment scheme to support the various applications requirement. Note that the ISR AP does not support access point repeater and WGB.

Advanced Encryption Standard (AES) – CCMP

This feature supports Wi-Fi Protected Access (WPA2) which is the Wi-Fi Alliance specification for interoperable wireless LAN security that supports IEEE 802.11i authentication and AES-CCMP encryption.

Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) is an authentication protocol for the 802.1X framework for mutual authentication between the client and a RADIUS server. New EAP authentication types supported in this IOS release include EAP-TTLS, EAP-MD5, and EAP-SIM.

IEEE 802.1X Local Authentication Service for EAP-FAST

This feature allows an IEEE 802.1X enabled RADIUS Server supporting EAP-FAST authentication types to run on Cisco IOS Software, thereby allowing the access point to authenticate wireless clients when the WAN link is down or the RADIUS Server at the central site is not available.

Microsoft WPS IE SSIDL

SSIDL Information Element support.

Multiple Basic Service Set ID (BSSID)

This feature permits a single AP to appear to the WLAN as multiple virtual APs. It does this by assigning an AP with multiple Basic Service Set IDs (BSSIDs) or MAC address. The AP is able to use a different BSSID to advertise each SSID and is therefore able to appear to WLAN clients as if there are multiple physical APs. Each BSSID/SSID combination advertised by the AP is able to be configured to support encrypted or unencrypted traffic.

NAC - L2 IEEE 802.1x

Network Admission Control (NAC) L2 IEEE 802.1x extends NAC support to layer 2 switches and wireless access points. Combining it with 802.1x provides a unified authentication and posture validation mechanism at the layer 2 network edge. This helps protect the network from attack by machines with insufficient antivirus posture. Performing posture validation at the edge maximizes the portion of the network which is protected and allows posture validation to be performed within a VLAN.

Universal Client Mode

This feature allows the access point radio to act as a client to another Cisco or Third-party access point. See caveats for known issues.

VLAN Assignment By Name

This feature provides the ability for the RADIUS server to assign an 802.11 client to a VLAN identified by NAME. Prior to the introduction of this feature, VLANs had to be identified by “VLAN_ID.”

Wi-Fi Multimedia (WMM) Required Elements

This feature supports WMM which is the Wi-Fi Alliance specification for QOS.

Wireless Non-Root Bridge

The wireless non-root bridge allows the access point radio to operate as the remote node in a point to point or point to multi-point network. See caveats for information on antenna support.

Wireless Root Bridge

The wireless root bridge role provides support for both point-to-point or point to multi-point bridging. See caveats for information on antenna support.

New Features in Release 12.4T

For information regarding the features supported in Cisco IOS Release 12.4T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com:

http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html

Caveats

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

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

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. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

Caveats for Cisco IOS Release 12.4(11)XJ

Open Caveats - Cisco IOS Release 12.4(11)XJ6

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ6

`CSCsh12480`

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

Cisco has released free software updates that address this vulnerability.

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

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

`CSCsg91306`

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

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

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

Open Caveats - Cisco IOS Release 12.4(11)XJ4

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ4

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.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

`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.

`CSCsi60004`

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

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

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

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

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

`CSCsi80749`

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

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

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

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

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

`CSCsh84171 Memory corruption in IOMEM - block overrun, FPGA ISDN DMA issue`

Symptom Router is crashing due to memory corruption with following message:
%SYS-3-OVERRUN: Block overrun at 3F379450 (red zone 2A2A2A2A)

Conditions This occurs on a 2800 router running 12.4T images.

Workaround There is no workaround.

```
CSCsi60919 HWIC-ADSL-B/ST or HWIC-1ADSL Ping Fails After External Shut/No Shut
```

Symptom ADSL stops receiving any more packet after external shut/no shut or ADSL line retrains several times. This is specific to HWIC-1ADSL, HWIC-1ADSLI, HWIC-ADSL-B/ST, and HWIC-ADSLI-B/ST.

Conditions It happens after external shut/no shut or ADSL line retrains 8 times.

shut/no shut the ADSL ATM interface.

Workaround There is no workaround.

```
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 web site at:
http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

```
CSCsi45826 When a call is made, display shows its own ephone-dn name
```

```
CSCsh89887 One way voice path with h/w conference on ephone-dn w/o preference 0
```

```
CSCsi46911 MALLOCFAIL failure on 2800,Cause: Mempool corrupt
```

Symptom While doing h323 to sip interop, the router is crashing due to Mempool corrupt.

Topology: PhoneA -- CME1 --- SIP --- CME2 -- PhoneB

Call flow:

1. PhoneA calls PhoneB.
2. PhoneB answers.
3. PhoneB presses transfer.
4. PhoneB presses NewCall.
5. PhoneB dials PhoneA.
6. We see PhoneB drop out of the call with no error indications or tones.
7. We see PhoneA display one call on hold and the other call incoming.
8. Hang up PhoneA.
9. PhoneA rings briefly when you put it on hook.

Workaround There is no workaround.

```
CSCsi65535 codec configured under ephone is used by all monitored phone.
```

Symptom The “codec” configuration under a “ephone” which monitors a line (“ephone-dn”) with the “m” button configuration command affects the codec of calls involving that “ephone-dn” as if the line was shared in the regular manner (using the “:” button configuration command).

Conditions Please see the “Symptom” description above. Please remember that the “codec” configuration under “ephone” is for phones registering over a WAN to the CME router. It directs CME to attempt to use the G.729 codec to save some bandwidth over that WAN segment, in some (non-VoIP) call scenarios. It doesn't restrict the codec of any call in any way. There is no well defined “negotiation” mechanism that makes use of this codec configuration as in H.323/H.245 codec negotiation for example.

Workaround There is no workaround.

```
CSCsi79331 Overlay DN gets stuck to BUSY when using loopbacked TCL script
invocation
```

Symptom Ephone dn gets stuck in a busy state.

Conditions Callers will get ringback but no phone will actually ring.

Workaround Remove the DN, then add it back in. Also have to add all the buttons for that DN back on the ephones.

```
CSCsi58842 CME: 7960+7914 display select line when conference IP phone
```

Symptom

1. A caller call a person "A".
2. Person "A" answer the call.
3. Person "A" is monitored by the person "B".
4. The person "B" see on his phone that the person "A" has received a call. Also person "B" calls person "A" using the monitor button.
5. Person "A" answers the call, putting the first caller on hold.
6. Person "A" uses the conference softkey "Confirm".
7. The message "Select Line" appears without any effect.

Workaround There is no workaround.

```
CSCsi14143 Some phone types not working with trunk monitor lines
```

Symptom The 7920, 7921, and 7985's line icon change does not change in response to a seized trunk line.

Conditions A 7920, 7921, or 7985's line is configured under CME with 'trunk <xxx> monitor-port x/x/x' and the corresponding trunk is seized.

Workaround There is no workaround.

```
CSCsi04538 Router crash with memory corruption when configure cert-upgrade auth
mod
```

Symptom A router that is configured as a Cisco Unified Call Manager Express (CUCME) router may crash because of a memory corruption.

Conditions This symptom is observed when voice calls are made involving a transcoder.

Workaround There is no workaround.

`CSCsg38919 Traceback and DSP timeout found after T1/E1 CAS call is established`

`CSCek74685 Wrong caller ID showed on XEE after Consult Transfer`

Symptom When SIP phone calls through SIP trunk to (XOR) phone and transfer to another (XTO) phone, the XTO phone shows the XOR caller id.

`CSCsf02356 <calling-number local> is broken for hairpin call forwarding`

Symptom Calling party information is shown wrongly for a forwarded call when using 'calling-number local'.

Conditions On CME 4.0 configured with 'calling-number local', a forwarded call rings the forward target and displays calling party name, number and redirection information. When 'calling-number local' is configured, the call setup to the forwarding target should just contain the forwarder's name and number as calling party information.

Workaround There is no workaround.

`CSCsi41401 Spurious memory access at ephone_delete_tftp_binding_by_url`

Symptom Spurious memory access seen on startup or after creating cnf files.

Conditions CME secure phone config.

Workaround There is no workaround.

`CSCsi29899 Fast busy in CME 4.1 if two conferences completed at same time`

Symptom Creator of conference gets a fast busy when trying to complete conference. Other parties of potential conferenced are connected to parties of separate conference

Conditions User must have CME 4.1 using hardware resources for conferencing. Two users must try to complete separate conferences at same time

Workaround There is no workaround.

CSCsg96319 reverse ssh eliminated telnet authentication on VTY

Symptom Anyone can have unprivileged Telnet access to a system without being authenticated, when a reverse SSH session is established with valid authentication credentials. This only affects reverse SSH sessions where a connection is made with the **ssh -l userid**:*number ip-address* command.

Conditions This symptom has been seen only when Reverse SSH Enhancement is used. This enhancement is documented at the following URL: http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_rev_ssh_enhanmt_external_docbase_0900e4b1805b0676_4container_external_docbase_0900e4b1807b42a5.html

Workaround Configure reverse SSH with the **ip ssh port** *portno* **rotary** *rotarygroup* 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

CSCsi56172 CME 4.1 IP phone dropped when trying to complete hardware conference

Symptom IP phone trying to create an ad-hoc conference is dropped when pressing “Conf” softkey the second time.

Conditions Must be using hardware conferencing in CME 4.1. The IP phone must receive a call first on on overlaid button. This initial call must come in on any DN besides the first DN configured in the “button” command in ephone config.

CSCsg37315 IOS FW on VPN tunnels fail on 12.4(11)T on 87x and 18xx platforms

Symptom If CBAC is configured in conjunction with VPN tunnels, TCP connections through the firewall might fail. CBAC ignores the SYN/ACK packets coming from IPsec tunnel and then drops all outbound TCP packets except initial SYN, generating message “Invalid Segment tcp”. Outbound TCP connections to the Internet (not over IPSec tunnel) are not affected and work fine with CBAC.

Conditions VPN tunnels must be configured on the router in conjunction with CBAC

Workaround Disable hardware encryption on the router with the command: **no crypto engine accelerator**

CSCsi93064 Only One line is available in CME GUI for 7921 instead of SIX

Symptom When a 7921 IP Phone is in “registered” status, CME GUI displays only one line instead of six lines.

Conditions There is no workaround

Workaround Use the CLI to configure additional lines.

CSCsi07340 no call waiting notification for monitored line

CSCsh24266 L2TP connection fails on PPP phase due to invalid UDP port#

Symptom L2TP connection fails on PPP phase because the LNS replies PPP frame
within L2TP frame including invalid UDP destination port number, to LAC.

Conditions

- This problem only occurs on PPP phase after L2TP setup.
- On L2TP tunnel/session setup phase, LNS uses correct UDP port number.
- source port number which LNS generates is not affected.
- If you use Cisco router as LAC, this problem will not occur.

Workaround There is no workaround.

CSCsi78162 SNASw %DATACORRUPTION-1-DATAINCONSISTENCY messages

CSCsf96318 QSIG (ISO) Call back fails between 3745 and 1760

CSCsi13312 Authentication fails and unable to login to a factory fresh router

Symptom Authentication with Security Device Manager (SDM) 2.3.3 fails, preventing you from logging into the router through HTTPS, HTTP, SSH, Telnet, console, or any management application.

Conditions This symptom is observed on a Cisco router that is “fresh out of the box” and affects the following routers:

Cisco 800 series
Cisco 1700 series
Cisco 1800 series
Cisco 2700 series
Cisco 2800 series

Cisco 3700 series
Cisco 3800 series

Workaround For extensive information and a workaround, see the following Field Notice: http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

```
CSCsi39520 CME: SIP MWI relay does not send notify msg after MWI on from Unity
```

```
CSCsi94745 ISDN call is dropped in due to STATUS message from PBX
```

Symptom Call is dropped from GW in response to STATUS message from PBX.

Conditions Then CONNECT message has Channel ID i.e., some PBX complain and send STATUS message.

Workaround There is no workaround.

```
CSCse91298 Sharedline and Overlay Phone Calling the Sharedline Cause Port Hung
```

Symptom STCAPP port get hung in various state.

Conditions When a sharedline member calls the sharedline DN phone number, the other sharedline member which also overlay DNs on the same line will get port hung in various state.

Workaround Reload

```
CSCsi76991 incoming sip call transferred local; audio not heard on ip phone
```

Symptom After the call transfer on alert, audio is not heard on ip phone

Conditions G729 call from Service Provider Network through SIP trunk to IP phone A on CME, transferred local on alert (blind transfer) to ip phone B; CME is configured to hairpin the calls

Workaround There is no workaround.

Further Problem Description: During the call transfer, service provider network send slightly different media capabilities on the 200 OK with SDP; capabilities are agreed from CME; but this new capabilities seem to make the issue;

```
CSCse56501 two sockets(IP V4 and V6)  bound to the same UDP port not working.
```

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.

Open Caveats - Cisco IOS Release 12.4(11)XJ3

There are no open caveats in this release.

```
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.

```
CSCsi67763 memory leak under simpleudpfuzz attack for port 500
```

Symptom The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link: http://www.kb.cert.org/vuls/id/739224.

By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

Cisco response is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtm

```
CSCsh86912 HWIC-4SHDSL: Implement CO mode support and line probing (PMMS) config
```

Symptom Need to add a CLI to configure a HWIC-4SHDSL as CO and a CLI to configure the noise margin settings for auto mode.

Workaround This is an enhancement.

Further Problem Description:

```
Router(config)#controller shdSL 0/3/0
Router(config-controller)#termination ?
 co   termination co (network)
 cpe  termination cpe (customer)

Router(config-controller-dsl-group)#shd rate auto pmmsmargin ?
 current  PMMS Current SNR Margin
 worst    PMMS Worst SNR Margin
```

`CSCsi11217 HWIC-4SHDSL has issue on IMA interface w/Lucent SHDSL-IMA card`

Symptom Some links in IMA group are shown as down though they are active at IMA level.

Conditions With Lucent as DSLAM, when IMA group is made inactive and then active again, some links are shown as down and not counted as active.

Workaround Doing a shutdown/no shutdown from the CLI at the dsl group recovers from the issue.

`CSCsj23569 codec selection issue on incoming SIP trunk`

Symptom Incoming call on a SIP trunk with G729 as preferred codec sets up but there is no ringback and dtmf is not working.

Conditions

```
incoming SDP 18 0 8 101
!
voice class codec 729
codec preference 1 g729br8
codec preference 2 g729r8
codec preference 3 g711ulaw
!
```

Workaround Do not use voice-call codec.

`CSCsj03494 I/O Memory corruption crash with IP communicator and 7961 IP Phones`

Symptom A 2811 series router may crash due to I/O memory corruption.

Conditions Router running CME 4.1 with 12.4.11.XJ3 image and using IP communicator and/or IP phones

Workaround Stop using IP phones or IP communicator.

```
CSCsj18014 Caller ID string received with extra characters
```

Symptom Caller ID is received with extra characters.

Conditions Whatever name is sent by the source will be received by the destination.

Workaround There is no workaround.

```
CSCsh84171 Memory corruption in IOMEM - block overrun, FPGA ISDN DMA issue
```

Symptom Router is crashing due to memory corruption with following message:
%SYS-3-OVERRUN: Block overrun at 3F379450 (red zone 2A2A2A2A)

Conditions This occurs on a 2800 router running 12.4T images.

Workaround There is no workaround.

```
CSCsi60919 HWIC-ADSL-B/ST or HWIC-1ADSL Ping Fails After External Shut/No Shut
```

Symptom ADSL stops receiving any more packet after external shut/no shut or ADSL line retrains several times. This is specific to HWIC-1ADSL, HWIC-1ADSLI, HWIC-ADSL-B/ST, and HWIC-ADSLI-B/ST.

Conditions It happens after external shut/no shut or ADSL line retrains 8 times.
shut/no shut the ADSL ATM interface.

Workaround There is no workaround.

```
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/en/US/docs/ios/12_4/12_4x/release/notes/rn1800xj.html

```
CSCsi45826 When a call is made, display shows its own ephone-dn name
```

```
CSCsh89887 One way voice path with h/w conference on ephone-dn w/o preference 0
```

```
CSCsi46911 MALLOCFAIL failure on 2800,Cause: Mempool corrupt
```

Symptom While doing h323 to sip interop, the router is crashing due to Mempool corrupt.

topology:

phoneA -- CME1 --- SIP --- CME2 -- phoneB

call flow:

phoneA calls phoneB
phoneB answers.
phoneB presses xfer.
phoneB presses NewCall.
phoneB dials phoneA.
We see phoneB drop out of the call with no error indications or tones.
We see phoneA display one call on hold and the other call incoming.
hang up phoneA.
phoneA rings briefly when you put it on hook.

results:

repeated this test four times.

Workaround There is no workaround.

```
CSCsi65535 codec configured under ephone is used by all monitored phone.
```

Symptom The “codec” configuration under a “ephone” which monitors a line (“ephone-dn”) with the “m” button configuration command affects the codec of calls involving that “ephone-dn” as if the line was shared in the regular manner (using the “:” button configuration command).

Conditions Please see the "Symptom" description above. Please remember that the "codec" configuration under "ephone" is for SCCP phones registering over a WAN to the CME router. It directs CME to attempt to use the G.729 codec to save some bandwidth over that WAN segment, in SOME (non-VoIP) call scenarios. It doesn't restrict the codec of any call in any way. There is no well defined “negotiation” mechanism that makes use of this codec configuration as in H.323/H.245 codec negotiation for example.

Workaround There is no workaround.

```
CSCsi79331 Overlay DN gets stuck to BUSY when using loopbacked TCL script
invocation
```

Symptom Ephone dn gets stuck in a busy state

Conditions Callers will get ringback but no phone will actually ring

Workaround Remove the DN, then add it back in. Also have to added all the buttons for that DN back on the ephones

```
CSCsi58842 CME: 7960+7914 display select line when conference IP phone
```

Symptom
*Apr 4 15:20:08.924: ephone-1[2][SEP0013C461B7D0]:Conference with line 1 DN 7 chan 1 on-hold
*Apr 4 15:20:08.924: ephone-1[2]:DisplayMessage: Silectionner la ligne ==> Select line option appears. Customer trys to select the line onhold and nothing happens. After 6 sec I assume a timeout is reached and the call disconnects.
*Apr 4 15:20:14.180: ephone-1[2]:ONHOOK (from phone msgID=7)===> this when the problem happens
*Apr 4 15:20:14.180: ephone-1[2]:ClearCallPrompt line 1 ref 21
*Apr 4 15:20:14.184: ephone-1[2][SEP0013C461B7D0]:CallPrompt line 1 ref 21:
*Apr 4 15:20:14.184: ephone-1[2]:
bulk_speeddial_init_ephone: 0

1. A caller call a person "A"
2. The person "A" answer the call
3. The person "A" is monitored by the person "B"
4. The person "B" see on his phone that the person "A" has received a call, also the person "B" call "A" using the monitor button.
5. The person "A" answer the call, pushing the first caller on hold.
6. The person "A" use the conference softkey "Confrn".

7. The message "Select Line" appear without any effect.

Workaround There is no workaround.

CSCsi14143 Some phone types not working with trunk monitor lines

Symptom The 7920, 7921, and 7985's line icon change does not change in response to a seized trunk line.

Conditions A 7920, 7921, or 7985's line is configured under CME with 'trunk <xxx> monitor-port x/x/x' and the corresponding trunk is seized.

Workaround There is no workaround.

CSCsi14143 Some phone types not working with trunk monitor lines

Symptom The 7920, 7921, and 7985's line icon change does not change in response to a seized trunk line.

Conditions A 7920, 7921, or 7985's line is configured under CME with 'trunk <xxx> monitor-port x/x/x' and the corresponding trunk is seized.

Workaround There is no workaround.

CSCsi04538 Router crash with memory corruption when configure cert-upgrade auth mod

Symptom A router that is configured as a Cisco Unified Call Manager Express (CUCME) router may crash because of a memory corruption.

Conditions This symptom is observed when voice calls are made involving a transcoder.

Workaround There is no workaround.

CSCsg38919 Traceback and DSP timeout found after T1/E1 CAS call is established

CSCek74685 Wrong caller ID showed on XEE after Consult Transfer

Symptom When SIP phone calls through SIP trunk to SCCP(XOR) phone and transfer to another SCCP(XTO) phone, the XTO SCCP phone shows the XOR caller id.

CSCsf02356 <calling-number local> is broken for hairpin call forwarding

Symptom Calling party information is shown wrongly for a forwarded call when using 'calling-number local'.

Conditions On CME 4.0 configured with 'calling-number local', a forwarded call rings the forward target and displays calling party name, number and redirection information. When 'calling-number local' is configured, the call setup to the forwarding target should just contain the forwarder's name and number as calling party information.

Workaround There is no workaround.

CSCsi41401 Spurious memory access at ephone_delete_tftp_binding_by_url

Symptom Spurious memory access seen on startup or after creating cnf files.

Conditions Conditions: CME secure phone config.

Workaround There is no workaround.

CSCsi29899 Fast busy in CME 4.1 if two conferences completed at same time

Symptom Creator of conference gets a fast busy when trying to complete conference. Other parties of potential conferenced are connected to parties of separate conference

Conditions User must have CME 4.1 using hardware resources for conferencing. Two users must try to complete separate conferences at same time

Workaround There is no workaround.

```
CSCsg96319 reverse ssh eliminated telnet authentication on VTY
```

Symptom Anyone can have unprivileged Telnet access to a system without being authenticated, when a reverse SSH session is established with valid authentication credentials. This only affects reverse SSH sessions where a connection is made with the **ssh -l userid**:*number ip-address* command.

Conditions This symptom has been seen only when Reverse SSH Enhancement is used. This enhancement is documented at the following URL: http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_rev_ssh_enhanmt_external_docbase_0900e4b1805b0676_4container_external_docbase_0900e4b1807b42a5.html

Workaround Configure reverse SSH with the>**ip ssh port** *portno* **rotary**<noCmdBold> *rotarygroup* 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

```
CSCsi56172 CME 4.1 IP phone dropped when trying to complete hardware conference
```

Symptom IP phone trying to create an ad-hoc conference is dropped when pressing "Conf" softkey the second time.

Conditions Must be using hardware conferencing in CME 4.1. The IP phone must receive a call first on on overlaid button. This initial call must come in on any DN besides the first DN configured in the “button” command in ephone config.

```
CSCsg37315 IOS FW on VPN tunnels fail on 12.4(11)T on 87x and 18xx platforms
```

Symptom If CBAC is configured in conjunction with VPN tunnels, TCP connections through the firewall might fail. CBAC ignores the SYN/ACK packets coming from IPsec tunnel and then drops all outbound TCP packets except initial SYN, generating message "Invalid Segment tcp". Outbound TCP connections to the Internet (not over IPSec tunnel) are not affected and work fine with CBAC.

Conditions VPN tunnels must be configured on the router in conjunction with CBAC

Workaround Disable hardware encryption on the router with the command: **no crypto engine accelerator**

```
CSCsi93064 Only One line is available in CME  GUI for 7921 instead of SIX
```

Symptom When a 7921 IP Phone is in “registered” status, CME GUI displays only one line instead of six lines.

Conditions There is no workaround

Workaround Use the CLI to configure additional lines.

```
CSCsi07340 no call waiting notification for monitored line
```

```
CSCsh24266 L2TP connection fails on PPP phase due to invalid UDP port#
```

Symptom L2TP connection fails on PPP phase because the LNS replies PPP frame within L2TP frame including invalid UDP destination port number, to LAC.

Conditions
- This problem only occurs on PPP phase after L2TP setup.
- On L2TP tunnel/session setup phase, LNS uses correct UDP port number.
- source port number which LNS generates is not affected.
- If you use Cisco router as LAC, this problem will not occur.

Workaround There is no workaround.

```
CSCsi78162 SNASw %DATACORRUPTION-1-DATAINCONSISTENCY messages
```

```
CSCsf96318 QSIG (ISO) Call back fails between 3745 and 1760
```

```
CSCsi13312 Authentication fails and unable to login to a factory fresh router
```

Symptom Authentication with Security Device Manager (SDM) 2.3.3 fails, preventing you from logging into the router through HTTPS, HTTP, SSH, Telnet, console, or any management application.

Conditions This symptom is observed on a Cisco router that is "fresh out of the box" and affects the following routers:

Cisco 800 series
Cisco 1700 series
Cisco 1800 series
Cisco 2700 series
Cisco 2800 series

Cisco 3700 series
Cisco 3800 series

Workaround For extensive information and a workaround, see the following Field Notice: http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

`CSCsi39520 CME: SIP MWI relay does not send notify msg after SCCP MWI on from Unity`

`CSCsi94745 ISDN call is dropped in due to STATUS message from PBX`

Symptom Call is dropped from GW in response to STATUS message from PBX.

Conditions Then CONNECT message has Channel ID ie, some PBX complain and send STATUS message.

Workaround There is no workaround.

`CSCse91298 Sharedline and Overlay Phone Calling the Sharedline Cause Port Hung`

Symptom STCAPP port get hung in various state.

Conditions When a sharedline member calls the sharedline DN phone number, the other sharedline member which also overlay DNs on the same line will get port hung in various state.

Workaround Reload

`CSCsi76991 incoming sip call transferred local; audio not heard on ip phone`

Symptom After the call transfer on alert, audio is not heard on ip phone

Conditions G729 call from Service Provider Network through SIP trunk to skinny IP phone A on CME, transferred local on alert (blind transfer) to skinny ip phone B; CME is configured to hairpin the calls

Workaround There is no workaround.

Further Problem Description: During the call transfer, service provider network send slightly different media capabilities on the 200 OK with SDP; capabilities are agreed from CME; but this new capabilities seem to make the issue;

```
CSCse56501 two sockets(IP V4 and V6)  bound to the same UDP port not working.
```

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.

```
CSCsi84017 c2600 router hangs during reload
```

Symptom When a c2600 router is loaded with the c2600-entservices-mz.124-9.T4 image, the router hangs during reload.

Conditions The problem occurs when a c2600 router is loaded with c2600-entservices-mz.124-9.T4 image, the router hangs during reload.

Workaround There is no workaround.

```
CSCsh84117 Memory corruption in IOMEM - block overrun, FPGA ISDN DMA issue
```

Symptom A router that is configured with an HWIC-ADSL-B/ST crashes because of memory corruption and generates the following error message:

```
%SYS-3-OVERRUN: Block overrun at 3F379450 (red zone 2A2A2A2A)
```

Conditions This symptom is observed on a Cisco 2800 series that runs Cisco IOS Release 12.4T.

Workaround There is no workaround.

```
CSCsg96319 reverse ssh eliminated telnet authention on VTY
```

Symptom When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the **ssh -l** *userid* **:** *number ip-address* command.

Conditions This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:
http://www.cisco.com/en/US/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

```
CSCsi76991 incoming sip call transferred local; audio not heard on ip phone
```

Symptom After a call is transferred on alert, audio is not heard on IP phones.

Conditions When a G729 call from a Service Provider Network through a SIP trunk to SCCP IP phone A on CME is transferred local on alert (blind transfer) to SCCP IP phone B; CME is configured to hairpin the calls.

Workaround There is no workaround.

Further Problem Description: During the call transfer, the service provider network sends slightly different media capabilities on the 200 OK with SDP; these capabilities are agreed upon from CME; but this new capabilities seems to cause this problem.

```
CSCsj04361 W button may not be lit on
```

Symptom The W button is not lit on when the watched phone goes off hook.

Conditions This problem only occurs after the CME reboots and the watched phone has speed-dial button configured.

Workaround Reset the watched phone. Restart the watched phone. Remove the speed-dial button.

```
CSCek76902 Router with ISDN interface may crash - Bus Error at CCPRI_AcceptChanId
```

Symptom Router with ISDN interfaces may crash with a bus error.

Conditions Router is running an IOS image that has CSCef58974 integrated. A specific Q.931 SETUP message is received for a preferred channel which is not available.

Workaround There is no workaround.

`CSCsg62638 CPU usage reaches 99% after nmap scan on port 53`

Symptom Scan of a router when a DNS server is enabled can cause high CPU usage of the DNS process itself. Overall performance of the device can deteriorate to some extent.

Conditions This symptom has been observed on a router when a DNS server is enabled when running Cisco IOS software from Cisco IOS Release 12.4 (11.1)T up to but not including Cisco IOS Release 12.4(13.08)T.

Workaround The only way to rectify this situation is to reboot the device.

Further Problem Description Upgrading the software is suggested.

`CSCse80323 modify component build system to support qnx and freescale processors`

Symptom The cbs did not support qnx.

Conditions The cbs was modified to support qnx by the addition of qnx object contexts. in addition the cbs was modified to allow the override of gcc with qcc.

Workaround In order to use qnx with the cbs, modify the makefile to specify qnx.all or qnx.[processor type] in the objects variable.

`CSCsj32707 GW rejects SIP UPDATE with Cseq 0`

Symptom A `SIP UPDATE` message from a Cisco CallManager or SIP Proxy Server with a `Cseq` value of 0 may be rejected or considered invalid by A Cisco gateway.

Conditions This symptom is observed on a Cisco gateway that runs Cisco IOS Release 12.4(9)T4 or a later release and that is connected to a SIP endpoint.

Workaround There is no workaround.

Note The symptom does not occur in Cisco IOS Release 12.4(9)T3.

CSCsh34690 Commit cflow patches for source files and link maps to all branches

Symptom Cflow instrumentation requires definitions of constructors. If it is not defined the build fails with the following error: Undefined reference to __CTOR_INIT__ Few *.link files in the platform directory gets patched during cflow build.

Conditions This patching happens only when the cflow build is done using dpe-cli tool.

Further Problem Description Extra time is spend by the dpe-cli tool to checkout-patch and again undo-checkout while exiting. Also since this checkout-patches happens during every build, modified files will be compiled and linked every time. This extra processing can be reduced by checking-in the changes to the branches.

CSCsb79076 MGCP RSVP enabled calls fails due to spurious error @ qosmodule_main

Symptom Errors and tracebacks are observed while making MGCP RSVP calls on a analog (RGW) setups. Observed in 12.4(3.9)T1 IOS version.

Workaround There is no workaround.

CSCsi39520 CME: SIP MWI relay does not send notify msg after SCCP MWI on from Unity

Symptom CME does not send the necessary SIP notify message to remote CME systems following the receipt of a valid SCCP mwi on message from Unity or Unity Connection even though the remote phones are properly listed in **show mwi relay clients** command.

MWI works correctly for phones on CME1. Phones on CME2 can subscribe and show up in **show mwi relay clients** command however no notify is sent in response to messaging from Unity.

Workaround Use Cisco IOS Release 12.4(4)XC6 or Cisco IOS Release 12.4(4)T7.

CSCsi84335 tracebacks observed in parseCallerIDString

Symptom When testing hsi performance with cps=50 and CHT=180. The GW main will core dump:

```
-rw-------   1 root     root     584659614 Mar 21 12:30 core.25935_0_GWmain_1174451419
-rw-------   1 root     root     584659614 Mar 21 18:00 core.26122_0_GWmain_1174471233
bash-3.00$
```

Conditions This is a performance tes.t

Workaround There is no workaround.

```
CSCek75251 repeat fix of damage
```

```
CSCse93722 change component build system to suppoprt the generation of shared objs
```

```
CSCsh53643 mbar/isync compiler automation
```

```
CSCsh77241 Reverting the compiler back to c2.95.3-p11b
```

Open Caveats - Cisco IOS Release 12.4(11)XJ3

There are no open caveats for this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ3

`CSCsd85587`

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

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

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

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

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

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

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

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

Open Caveats - Cisco IOS Release 12.4(11)XJ2

```
CSCsi09530 CME SIP phone failed to register because of authenticate register
```

Symptom If “authenticate register” is configured under “voice register global”, CME SIP failed to registered.

Conditions “authenticate register” is configured under “voice register global”, when CME is acting as a RIGISTRAR

Workaround Disable “authenticate register” under “voice register global”

Further Problem Description: In registrar Functionality, CME challenges an inbound Register request with 401 response If “authenticate register” is configured under “voice register global”. The Registering Endpoint then Sends a Register Request with Crdentials. GW Stack is not processing this Request and is dropping it.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ2

```
CSCec12299
```

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

Workarounds are available to help mitigate this vulnerability.

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

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

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

```
CSCsf08998
```

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

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

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

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

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

```
Csg51259 CME: DTMF stops working after consult transfer to called party’s mailbox
```

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

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

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

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

```
CSCsg59037 85x/87x 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. Please consult this link for more information:

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

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

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

Workaround Unless removing the dialplan-pattern, no work around present.

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

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

Workaround Use b2b mode

```
CSCsg17289 DNS-SRV issues for SIP registrations
```

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

```
CSCsg18902 Blind transfer is not working on SIP trunk
```

Symptom Blind transfer failed on SCCP endpoint over SIP trunk

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

Workaround There is no workaround.

```
CSCse89321 Dtmf path not getting confirmed in sip media forking call
```

```
CSCsh23992 IAD2801 BRI voice port ISDN status does not come up
```

```
CSCsg94873 One way audio for PSTN to AA and calls xferred to SIP phone with G.729
```

```
CSCsh25511 A router may crash with CPU Vector 300
```

Symptom A router may crash with CPU vector 300

Conditions IOS running qos and cce

Workaround There is no workaround.

```
Further Problem Description:
```

```
CSCsh45544 Placed call list in 7970 phone always shows unknown number
```

```
CSCsh37177 %SDP-3-SDP_PTR_ERROR traceback error when redirecting call to AA
```

```
CSCsg31719 Digits are not relayed correctly when call is not connected.
```

Symptom When onhook dialing or speed dial is performed from CME to an analog port where dialtone is slightly delayed some digits are dropped.

Conditions This is not seen when the digits are delayed, or when the user waits to hear dialtone then dials.

Workaround Dial digit by digit

```
CSCsh14247 Call transfer fails when initiated from SIP Phone
```

```
CSCsg49416 Refer is not sent by CME when Cfwd all is set from TNP phone
```

```
CSCsh19990 Traceback= 0x438662AC 0x40BF2BEC with Call Park/Pick Up operation
```

```
CSCsh37345 DSL Operating-mode ‘auto tone low’ enables ETSI mode only
```

Symptom The DSL line fails to train with “dsl operating-mode auto tone low” command if the DSLAM does not support ETSI mode.

Conditions In the command **dsl operating-mode auto tone low**, the “**dsl operating-mode auto**” is used to enable all the supported modes on a DSL line and the “**tone low**” is used to disable DT-UR2 so that the DSL line can use the carrier tones 29 through 48. Instead, this command does not disable DT-UR2 and enables only ETSI mode. With this,

a. If the DSL configuration on the DSLAM does not support ETSI mode, then the DSL line fails to train up.
b. If the DSLAM supports ADSL2+, ADSL2, ETSI modes, then it trains in ETSI mode, where it's supposed to train in ADSL2+, since the ADSL2+ has higher priority than ETSI mode.

Workaround Avoid using “**dsl operating-mode auto**” command. To select a desirable mode along with disabling DT-UR2, the commands like “**dsl operating-mode adsl2+ tone low**” or “**dsl operating-mode adsl2 tone low**” can be used.

```
CSCsh11146 Memory leak at AFW_SS_SIP_PrepareTransferSetup
```

Symptom Memory leak occurred in transfer scenarios.

Workaround There are no workarounds.

```
CSCek67638 include presence feature in c2801 security package
```

Symptom The 2801 security image does not have presence feature.

```
CSCsh59469 DTMF is distorted when played from SCCP controlled ATA on CME
```

Symptom DTMF generated by a SCCP controlled ATA registered to CallManager Express may be choppy, broken, or overlapping when multiple digits are pressed, one after another.

Example topology:

```
IVR---fxs---ATA---sccp---CME---pri---PSTN
```

A user in the PSTN calls the IVR. The digits are not reliably detected by the IVR when pressed by the PSTN user because of the overlapping / choppy output.

Conditions This is seen on a SCCP controlled ATA registered to CallManager Express.

Workaround Use H323 software on the ATA.

```
CSCsh55262 Update CME GUI version and new Cisco logo
```

```
CSCsg95736 MAC address is missing for radio interface
```

Symptom IOS image is not reading the mac address for radio interface.

Workaround The problem is not seen if the dot11 interface is in up state.

```
CSCsh53808 Transcoder fails after several H.323 transcoded calls to CUE
```

```
CSCsg31559 Spurious memory access at strncmp, skinny_hwconf_check_adhoc_register
```

```
CSCsh14101 503 Service Unavailable should be sent to CAC rejected calls
```

```
CSCsh60218 VG224 continues to ring when first of two ringing shared calls hangs up
```

```
CSCsh48646 FAC fails for the first time after enabling in certain conditions
```

```
CSCsh78605 Need CLI to enable/disable SIP Line incoming dial-peer matching
```

Symptom For an inbound call across a SIP Trunk, IOS might match an dynamically configured dial-peer instead of the user-defined dial-peer configured with “incoming called-number“.

Conditions This problem was observed when IOS SIP Gateway was also configured as a SIP SRST.

Workaround Use IOS 12.4(6)T6.

```
CSCsh39749 Few objects of hdsl2ShdslSpanStatusTable giving wrong values with
ARCHER
```

Symptom MIB value for LineRate (hdsl2ShdslStatusMaxAttainableLineRate) queried through SNMP GET/GETNEXT returns incorrect values. Also hdsl2ShdslInvVendorID displays data in wrong format.

Conditions No Specific conditions.

Workaround For hdsl2ShdslStatusMaxAttainableLineRate, multiply the value with 1000 and for **hdsl2ShdslInvVendorID**, convert the displayed values into ASCII characters.

```
CSCsh63545 ARCHER IMA MIB modifications
```

Symptom SNMP walk on imaLinkIntervalTable returns no entries. SNMP get does not work for **imaGroupTable**.

Conditions No specific condition.

Workaround No workaround for **imaLinkIntervalTable**. Do a SNMP Walk on **imaGroupTable** to view the individual table entry values.

```
CSCsh46622 HDSL2-SHDSL-LINE-MIB:Few tables not populated for ARCHER with CRUSHER
on
```

Symptom When HWIC-4SHDSL and WIC-1SHDSL-V2 are present in a router, HDSL2-SHDSL-LINE-MIB entries for HWIC-4SHDSL are not getting displayed.

Conditions This problem happens if WIC-1SHDSL-V2 comes up before HWIC-4SHDSL.

1. Shutdown both HWIC-4SHDSL and WIC-1SHDSL-V2.
2. Reload the router. Do a “no shutdown” on HWIC-4SHDSL controller first and then do a “no shut” for WIC-1SHDSL-V2 controller.
3. Then save the config.

```
CSCsh41397 SNMP getone gives NO_SUCH_INSTANCE_EXCEPTION error for HWIC-4SHDSL
```

Symptom SNMP GET operation on HDSL2-SHDSL-LINE-MIB objects returns no such instance for HWIC-4SHDSL.

Conditions No specific conditions. The failure always happens when a SNMP get is done.

Workaround Workaround is to do SNMP Walk for the entire table.

```
CSCsh68584 CME MWI notify message not compliant to RFC 3842
```

Symptom MWI lights on 7970 does not glow

Conditions 7970 when configured as SIP phone for CME.

Workaround There are no workarounds

CSCsh68560 CME: sip to sccp to sccp attend transfer fails

Symptom One way audio.

Conditions The problem is observed when you have XEE SIP line or trunk, XOR and XTO sccp on same CME, consultation transfer.

Workaround No apparent workaround, except that the problem is intermittent.

```
CSCsh22682 vlan information disappears after router reload
```

Symptom Devices in data VLAN on MVAP configured port with portfast loose connectivity

Conditions Device is connected to MVAP configured port with portfast enabled. Router has been reloaded.

Workaround Remove and add data VLAN from VLAN database. Sometimes this does not seem to work

12.4(9)T and earlier releases do not see this problem

Do not use portfast on MVAP port

Further Problem Description: After the router has been reloaded we see an incomplete **arp** entry. Removing and adding VLAN data fixes this issue for a while. This issue is also resolved If the MVAP port does not have portfast enabled.

```
CSCsg76281 CME 4.1:PSTN-to-AA, tx to sccp1, then tx to sccp2, cfwd all to CUE fails
```

CSCsg18481 Consult Transfer failed with Call forward busy

Symptom Consult transfer failed when XTO has call-forward busy

Conditions XEE is SCCP endpoint and XOR is SIP phone

Workaround There are no workarounds

CSCsh58082 SIP: A router may reload due to SIP traffic

Symptom Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP. There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workaround Workarounds exist to mitigate the effects of this problem on devices which do not require SIP. This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.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

!

CSCsh95740 CME tftp bindings corrupt/erroneous with perphone cnf

Symptom On 12.4(11)XJ, performing a ‘show tele tftp-bindings’ may show corrupted or incorrect output.

Conditions The CME system was reloaded with ‘cnf-file perphone’ configured under telephony-service.

Workaround There is no workaround.

CSCek68607 CallerID not updated with AA CFB call to sip phone over SIP trunk

CSCsh90148 SIP UPDATE message sending should be controllable via CME on SIP trunk

Symptom UPDATE messages being sent on the SIP trunk cause calls to fail under certain conditions

Conditions Calls are over a SIP trunk from CME 4.1 to service provider SIP proxy

Workaround There are no workarounds

CSCsh45568 Alignment errors in classify_packet

Symptom Alignment errors may be seen on a Cisco router due to NBAR. High CPU may be seen as well.

Workaround No known workaround at this time.

CSCsf25671 Client with L2TPv2 on Virtual-PPP fails to get ip add from LNSs ip pool

Symptom L2TPv2 VPDN sessions are terminated by the client shortly after IPCP negotiation completion

```
00:00:23.859: Vp1 IPCP: State is Open
00:00:23.859: Vp1 IPCP: Install negotiated IP interface address #.#.#.#
00:00:23.859:  IP-ADDR: ip_new_address(), old 0.0.0.0/0, new #.#.#.#/# on
Virtual-PPP1
00:00:23.859: ACLIB [Vp1, 22]: ac_ppp_voluntary_restore_link_vectors() -
Restoring previously saved link
00:00:23.859: ACLIB [Vp1, 22]: SW AC interface UNPROVISIONED for PPP interface
Vp1
00:00:23.859: ACLIB: Unbinding SWSB subblock
00:00:23.859: ACLIB [Vp1, 22]: Deleting AC sublock structure.
00:00:23.859: ACLIB: ac_ppp_restart_session() - restarting LCP.
00:00:23.859: Xconnect[ac:Vp1(PPP)]: provisioning fwder with fwd_type=1,
sss_role=2
00:00:23.859: ACLIB: Setting new AC state to Ac-Provisioning, old state was
```

```
Ac-Idle
00:00:23.859: ACLquest
00:00:23.859:  IP-ADDR: invoke_ip_address_change() to 0.0.0.0/0, secondary

off, sense off, on Virtual-PPP1
00:00:23.859:  IP-ADDR: invoke_ip_address_change() to #.#.#.#/#, secondary

off, sense on, on Virtual-PPP1
00:00:23.859:  IP-ADDR: ipaddr_table_insert() #.#.#.#, in global table on

Virtual-PPP1IB [Vp1, 22]: AC attached subblock to Virtual-PPP1
00:00:23.859: ACLIB ive <Circuit Provisioned> msg
00:00:23.863: ACMGR [Vp1, 22]: provision event, FSP down state no chg, action

is ignore[Vp1, 22]: AC provisioned. Bringing down existin
00:00:23.863: XC L2TP: Received L2TUN API message <Unprovision>
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] Event <L2TUN Session Unprovision>,

state Established -> Established
00:00:23.863: XC L2TP: Sending L2TUN message <Disconnect>
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] L2TUN socket teardown:
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#]   "xconnect destroyed"
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] PW-MGMT: PW peer #.#.#.#, vcid #
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] PW-MGMT: Reason [Unprovisioned]g

PPP session on interface Vp1
00:00:23.859: ACLIB [Vp1, 22]: ac_ppp_voluntary_set_link_vectors() changing

vectors for Vp1
00:00:23.859: ACLIB [Vp1, 22]: SW AC intf PROVISIONED for PPP interface Vp1
00:00:23.859: Xconnect[unkn:#.#.#.#:#]: provisioning fwder with fwd_type=2,

sss_role=1
00:00:23.859: XC L2TP: XConnect provision re
00:00:23.859: Vp1 IPCP: Install route to #.#.#.#
00:00:23.863: L2TP:(Tnl#:Sn#)L2X s/w switching session unboun #.#.#.# vcid #,

Unprovisioned, VC state UP
00:00:23.863: XC L2TP: uid:116[#.#.#.#/#] Tell MIB that PW peer #.#.#.#, vcid

1 is UP
00:00:23.863: L2TUN APP: uid:116handle/176170Destroying app session
00:00:23.863: XC L2TP: Received L2TUN API message <Provision>
00:00:23.863: XC L2TP: uid:121[#.#.#.#/#] PW-MGMT: PW peer #.#.#.#, vcid 1
00:00:23.863: XC L2TP: uid:121[#.#.#.#/#] PW-MGMT: Reason [Provisioned]d
00:00:23.863: L2TP   #:#:#   : Received a SSM L2TP segment down event
00:00:23.863: ACMGR [Vp1, 22]: Receive <Circuit Unprovisioned> msg
00:00:23.863: ACMGR [Vp1, 22]: unprovision event, SIP state chg both up to

end, action is peer service disconnect
00:00:23.863: ACMGR [Vp1, 22]: Sent a sip service disconnect
```

Conditions Client-initiated xconnect L2TPv2 sessions

Workaround The problem was not observed in 12.4(9)T2

CSCse78963 Adopt new default summer-time rules from EPA BADCODE BUG

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

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

Workaround A workaround is possible by using the clock summer-time configuration command to manually configure the proper start date and end date for daylight savings time. After the summer-time period for calendar year 2006 is over, one can for example configure: clock summer-time PDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00 (this example is for the US/Pacific time zone)

```
CSCsi06347 CLI for MOH should be displayed under voice-port
```

Symptom CLI for MOH is hidden

Conditions Happens when signal loopstart live-feed is configured under voice-port.

Workaround There are no workarounds.

```
CSCsh98465 INFO request not generated on hookflash
```

Symptom INFO request messages is generated properly on hookflash

Conditions This feature is broken in 12.4(11)XJ based image

Workaround Currently there is no workaround.

```
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:

```
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:

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

`CSCse98165 Mid-call invite not sent to OGW with nat symmetric check-media-src`

Symptom IPIP gateway does not send an to the Originating gateway when a mid-call invite is received from the terminating gateway The following is configured on the IPIP gateway

sip-ua

nat symmetric check-media-src

Workaround There are no workarounds.

`CSCsh74276 Counter for Lost packet not cumulative during a call`

Symptom Packet loss counter varies randomly.

Conditions Sequence number goes wild.

Workaround There are no workarounds.

`CSCek70160 UDP packet corrupted in SIP->H323 IPIPGW during T38 mode`

Symptom In fax1 -- OGW --sip--- IPIPGW -- h323 -- TGW --fax2 scenario, T38 fax fails.

Conditions When “dtmf-relay rtp-nte digit-drop” is configured on IPIPGW and T38 is sent from fax1 to fax2.

Workaround There are no workarounds

CSCsh67943 7301 fails on a T38 when configured as IPIPGW doing SIP - H323

Symptom In fax1 -- OGW --sip--- IPIPGW -- h323 -- TGW --fax2 scenario, T38 fax fails.

Conditions When TGW is using v123-21 image, IPIPGW using 12.4(9)T image, T38 fails.

Workaround There are no workarounds.

```
CSCsi09696 CME SIP missed quotation for aop parameter
```

```
CSCsi18104 SIP: 400 Bad Request for AA's REFER, and AA's transfer failed
```

Symptom Seeing "400 Bad Request" response for AA's "REFER" request, and AA's semi-attended transfer failed against XJ1 image.

Conditions This happens when AA/CUE is configured to use **dtmf-relay sub-notify**.

Workaround **xfer** works if AA/CUE uses **dtmf-relay sip-notify**.

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

Symptom The minimum after-hours login timer is 5 mins. 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 are no workarounds.

```
CSCsg31867 Router crashes on large ping pkts with IPSEC/NAT configured
```

Symptom A Cisco IOS router may experience a unexpected reload.

Conditions This problem occurs in IOS version 12.4(11)T and later when the router is configured with IPSec and NAT, and when it needs to fragment a large packet to be encrypted over the IPSec tunnel.

Workaround There is no known workaround at this time.

```
CSCsh33057 SPEs in stuck state after stress
```

Symptom SPEs may hang after voice calls have been processed. When you enter the clear spe command for the affected SPEs, the platform may reload unexpectedly.

Conditions These symptoms are observed on a Cisco AS5400 and Cisco AS5850.

Workaround There is no workaround to prevent the SPEs from hanging. When the SPEs hang, reload the platform to recover the SPEs.

`CSCsg46624 Router crashes on applying service policy on the atm subinterface`

Symptom Router crash

Conditions When a policy map is applied on the mohican point to point subinterface.

Workaround There are no workarounds.

`CSCsh16540 Router Crashes when encapsulation dot1Q <VC id is enabled`

Symptom A router crashes when you enter the encapsulation dot1q vlan-id command.

Conditions This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(12.7) and that is configured for MPLS. However, the symptom is platform-independent.

Workaround There is no workaround.

`CSCsh83836 C1700 Router crashes @ fpm_db_add_acl`

`CSCsg80097 Calling name in Facility sent via CCM Sip trunk does not appear on SIP CME`

`CSCsh11157 Memory leak at DestCaptureCallForward`

`CSCsg40247 T38 Fax Relay calls are going as Cisco Fax Relay`

`CSCsi15229 No memory available if qos and acl on router`

Symptom One or more of the following symptoms may occur. CPU HOGS, crashes, high cup, and/or memory allocation failures.

Conditions This problem is triggered when making configuration changes to an access list that is currently in use by a service policy.

Workaround Disable the service policy before make changes to its components.

`CSCsg14313 traceback seen while making conference/transcoder co_exist calls`

`CSCsg57002 SIP timer tree corruption is causing SIP gateway crash under load`

Symptom The SIP Gateway will crash when handling calls involving DTMF relay.

Conditions Following is the scenario that is causing the crash: sip-notify and sip-kpml are configured as DTMF relay mechanisms on both Cisco IOS Gateway and CCM. When a call is coming in from CCM onto the GW, because of a bug (CSCse72749), GW negotiates the DTMF mechanism as sip-notify whereas CCM negotiates the DTMF relay mechanism as sip-kpml. Subsequently, CCM sends subscribe request for KPML. GW accepts the KPML subscription and starts the respective KPML timers. Now when the call is terminated, Cisco IOS GW is cleaning up the data structures without stopping the KPML timers since the negotiated DTMF relay on Cisco IOS GW is sip-notify.

Workaround There are two workarounds:

1. Migrate to a Cisco IOS version which has CSCse72749 fix integrated.
2. Enable either sip-notify or sip-kpml on the Cisco IOS GW (do not enable both).

`CSCsg34501 Traceback from voice_reg_supports_utf8 is seen`

`CSCsb79829 call dropped when incoming invite with alert-info header`

`CSCsg92387 Calling name in Notify message does not appear on SIP-CME Phone`

`CSCsh17599 One way audio with Adhoc conference by CCM and 1 participant hangs up`

`CSCsg36224 DSPs not released when conference DN no. is directly dialed`

`CSCsh32714 Spurious memory access traceback at sipSPI_ipip_copy_channelInfo_to_sdp`

`CSCsh57237 router crashes immediately after enabling service policy`

Symptom Router crashes

Conditions Crash happens immediately or after a few seconds of applying service policy on the gigabit ethernet and atm pvc. The only commands executed after applying the service policy are write memory and show run.

Workaround There are no workarounds.

`CSCsi24620 Enable support for StationUnicodeCapableMsk feature bit`

Symptom UTF8 localized characters can not display on new generation phones, ex 7970, 7961 and etc.

Conditions When using phone load later than 8.0.x.

Workaround There are no workarounds.

Further Problem Description: If the locale on CME requires UTF8 encoding the character will not display correctly with 8.0.x and newer phone loads.

`CSCsh11907 Router crashes @` fair_queue_classify_wred

Symptom Router crashes after show policy-map command

Workaround There is no workaround.

`CSCsg03849 Spurious accesses traceback seen @` **AFW_Leg_CheckConsultSetup**

Open Caveats - Cisco IOS Release 12.4(11)XJ

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XJ

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

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

Workaround There is no workaround.

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

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

Workaround Remove the dialplan-pattern.

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

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

Workaround There is no workaround.

```
CSCsg17289 DNS-SRV issues for SIP registrations
```

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

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

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

Workaround There is no workaround.

```
CSCsg18902 Blind transfer is not working on SIP trunk
```

Symptom Blind transfer failed on SCCP endpoint over SIP trunk

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

Workaround There is no workaround.

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

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

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

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

Workaround There is no workaround.

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

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

Workaround There is no workaround.

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

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

Workaround Use b2b mode.

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

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

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

Workaround There is no workaround.

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

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

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

Workaround There is no workaround.

CSCsg51259 DTMF stops working after consult transfer to called party mailbox

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

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

Workaround There is no workaround.

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

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

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

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

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

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

```
CSCek37305 Cisco 7200 router crashes at get_hwidb_if_same
```

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

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

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

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

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

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

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

```
CSCek45272 NAT overload failing with static mappings
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Workaround There is no workaround.

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

Symptom Entry for Crackerjack PA missing from cefcModuleTable.

Conditions SNMPGet on the table is issued.

Workaround There is no workaround.

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

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

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

Workaround There is no workaround.

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

Symptom A serial link goes down.

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

Workaround There is no workaround.

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

Symptom IP address removal from a physical interface

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

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

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

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

Workaround There is no workaround.

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

Symptom A Cisco IOS router may experience a unexpected reload.

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

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

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

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

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

Workaround There is no workaround.

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

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

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

Workaround There is no workaround.

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

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

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

Workaround Use non-default route prefix.

```
CSCsg12813 Speech loss after receiving MDCX from PGW
```

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

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

Workaround There is no workaround.

```
CSCsg16186 SCMabort Event crash seen on NPE-G2
```

Symptom System may crash during bootup.

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

Workaround Reduce IO memory in the configuration.

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

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

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

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

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

Symptom A few inconsistent error message.

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

Workaround There is no workaround.

CSCsg38907 rip - redistribute static: redistributed prefixes have metric 16

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

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

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

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

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

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

Example:

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

access-list 103 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255

This occurs when the following is true:

1) ezvpn client is configured

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

3) NAT is configured

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

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

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

Conditions The router must be configured with crpyto PKI trustpoints.

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

```
CSCsg46546 Erroneous alerting during pickup with CSCek58324 scenario
```

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

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

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

```
CSCsg47834 NACK is observed for Open voice channel command
```

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

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

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

Workaround

1) Disable Transcoding

(or)

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

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

Example 1:

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

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

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

Example 2:

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

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

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

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

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

```
CSCsg48183 Unforeseen ARP request send from all interfaces
```

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

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

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

Workaround There is no workaround.

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

Symptom Router crashes loading the IOS signature package file

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

Workaround There is no workaround.

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

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

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

Workaround There is no workaround.

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

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

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

Workaround There is no workaround.

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

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

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

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

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

```
CSCsg70355 Adopt new default summer-time rules from Energy Policy Act of 2005
```

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

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

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

```
clock summer-time PDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00
```

(this example is for the US/Pacific time zone)

```
CSCsg73806 Runaway debugs: AFW_Module_ObjectCount pCallIndSs
```

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

```
AFW_Module_ObjectCount pCallIndSs 1
```

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

Conditions This is seen on voice routers.

Workaround There is no workaround.

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

Symptom Min hit or event count not resetting correctly

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

Workaround There is no workaround.

```
CSCsg90212 VSA Add code to handle CRNG failure interrupt
```

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

```
VSA encountered CRNG failure
```

Workaround There is no workaround.

Additional References

The following sections describe the documentation available for the Cisco 1800 series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents. Documentation is available in pdf or html form.

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

- Release-Specific Documents, page 63
- Platform-Specific Documents, page 64

Release-Specific Documents

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

- *Cross-Platform Release Notes for Cisco IOS Release 12.4(11)T*
- *Caveats for Cisco IOS Release 12.4* and *Caveats for Cisco IOS Release 12.4(11)T*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1800 series routers (fixed) are available on Cisco.com at the following location:

http://www.cisco.com/en/US/products/ps5853/index.html

Cisco IOS Software Documentation Set

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

Documentation Modules

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

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

Cisco Feature Navigator

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. Feature Navigator is available 24 hours a day, 7 days a week.

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

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

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

Open Source License Acknowledgements

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

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

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

Original SSLeay License:

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

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

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

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

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.