Release Notes for Cisco IAD2801 Series Integrated Access Devices with Cisco IOS Release 12.4(22)YB

First Released: January 27, 2009
Last Revised: October 28, 2010
Cisco IOS Release 12.4(22)YB8
OL-19006-09 Nineth Release

These release notes for the Cisco IAD2801 Series Integrated Access Devices describe the product-related enhancements provided in the Cisco IOS Release 12.4(22)YB releases. These release notes are updated as needed.

For a list of the applicable software caveats, see the "Caveats" section on page 7. See also *Caveats for Cisco IOS Release 12.4(22)T*, which is updated for every maintenance release.

Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* and *About Cisco IOS Release Notes*.

Contents

These release notes describe the following topics:

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

Introduction

The following Cisco IAD2801 models are supported:

- IAD2801-2BRI-A/K9- Fixed configuration router, with integrated PVDM2-8, HWIC-1ADSL, and 1 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot
- IAD2801-4BRI-A/K9- Fixed configuration router, with integrated PVDM2-16, HWIC-1ADSL, and 2 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot.
- IAD2801-4BRI-S/K9- Fixed configuration router, with integrated PVDM2-16, HWIC-4SHDSL, and 2 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot

The following cards are supported in the factory configurable HWIC slot on all models:

- HWIC-4ESW
- VIC-4FXS
- HWIC-AP-AG-E or HWIC-AP-G-E

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.4(22)YB8, see the "New and Changed Information" section on page 3.

System Requirements

This section describes the system requirements for the Cisco IOS Release 12.4(22)YB releases and includes the following sections:

Memory Requirements

Table 1 lists the memory requirements for the Cisco IOS feature sets on the Cisco IAD2801 in Cisco IOS Release 12.4(22)YB8. The Cisco IAD2801 uses a 32-MB Flash memory card.

Table 1 Cisco Release 12.4(22)YB8 Memory Requirements for the Cisco IAD2801 Series IAD

Platform	Feature Set	Software Image	Flash Memory (MB)	DRAM Memory (MB)	Runs From
Cisco IAD2801	Cisco IAD2801 IOS Advanced IP Services	ciad2801-advipservices k9-mz	64	256	RAM
Cisco IAD2801	Cisco IAD2801 IOS SP Services	ciad2801-spservicesk9-mz	64	256	RAM

Hardware Supported

Cisco IOS Release 12.4(22)YB8 supports the Cisco IAD2801 series IADs.

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 3.

For information about supported hardware for this platform and release, see the *Hardware/Software Compatibility Matrix* at:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Determining the Software Release

To determine the version of Cisco IOS software currently running on your Cisco IAD2801 series router, see *About Cisco IOS Release Notes* located at:
http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *About Cisco IOS Release Notes* located at:

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Feature Set Tables

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

New and Changed Information

The following sections list the new hardware products and software features supported by the Cisco IAD2801 in Cisco IOS Release 12.4(22)YB:

New Hardware Features in Cisco IOS Release 12.4(22)YB8

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB8

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(22)YB7

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB7

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(22)YB6

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB6

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(22)YB5

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB5

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(22)YB4

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB4

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(22)YB3

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB3

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(22)YB2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB2

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(22)YB1

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB1

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(22)YB

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(22)YB

There are no new software features in this release.

Limitations and Restrictions

The following limitations and restrictions apply to the Cisco IAD 2801 series

Fixed Configuration Platforms Supporting Specific Cards

TheCisco IAD2801 series are fixed configuration platforms with each slot supporting specific cards. Supported cards in each model are shown below:

Table 2 Supported cards in Cisco IAD2801 series

Platforms	Slot 0	Slot 1	Slot 2	Slot 3
IAD2801-2BRI-A/K9	VIC2-2BRI-NT/TE-P	HWIC-1ADSL	Not Available	LTD Option[1]
IAD2801-4BRI-A/K9	VIC2-2BRI-NT/TE-P	HWIC-1ADSL	VIC2-2BRI-NT/TE-P	LTD Option[1]
IAD2801-4BRI-S/K9	VIC2-2BRI-NT/TE-P	HWIC-4SHDSL	VIC2-2BRI-NT/TE-P	LTD Option[1]

1. LTD OPTION (Factory installable or Field Upgradable)

- HWIC-AP-AG-E and HWIC-AP-G-E
- HWIC-4ESW
- VIC-4FXS/DID

Unsupported Card Message

If any unsupported card is detected during the bootup, the following message appears:

"Card is not supported in slot 2. Please remove it."

This message appears for each unsupported card detected.

If any cards are not supported and **smart-init** is enabled, another message appears during bootup:

```
Smart Init is enabled
smart init is sizing iomem
 ID             MEMORY_REQ          TYPE
                  0X003AA110 public buffer pools
                  0X00211000 public particle pools
                  0X00020000 Crypto module pools
                  0X00120000 VPM buffer pools
0X05B3            0X000034A0 Card in slot 0
0X04C8            0X00077D00 Card in slot 1
0X05B3            0X00000000 UNKNOWN Card in slot 2
0X003A            0X00000000 Card in slot 3
                  0X000021B8 Onboard USB
```

Caveats

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

This section contains the following caveat information:

Open Caveats - Cisco IOS Release 12.4(22)YB8

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(22)YB8

`CSCtj62596 Mismatched codecs cause one-way audio.`

Symptom One-way audio on certain call flows with SRTP.

Conditions Mismatch of SRTP keys.

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 12.4(22)YB7

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(22)YB7

CSCtj15884 One way voice/incorrect SRTP key handling.

Symptom One way voice when SRTP is used.

Conditions Interworking with PGW.

Workaround There is no workaround.

CSCsz72591 Router configured as a DHCP client crashes with crafted DHCP packet.

Symptom A router crashes with an Address Error (load or instruction fetch) exception.

Conditions The router must be configured to act as a DHCP client.

Workaround There is no workaround.

CSCsu47486 Cisco IOS Software configured with MGCP may reload.

Symptom Cisco IOS Software configured with MGCP may reload.

Conditions This symptom is observed if an authenticated user repeatedly configures **mgcp block-newcall** and **no mgcp block-newcall** while active calls are being made.

Workaround Wait for all active calls to terminate before configuring **no mgcp block-newcall**.

CSCsw64971 NAT-Entry deletion fails in SNAT backup router for H.323 RAS traffic.

Symptom NAT-Entry deletion fails in SNAT backup router for H.323 RAS traffic. Standby router also crashes if the Active interface is brought up.

Conditions This can occur when using SNAT with HSRP and has been seen on numerous images.

Workaround There is no workaround.

CSCtb73450 L2TPv3: SCCRQ packets causes tunnel to reset after digest failure.

Symptom Start-Control-Connection-Request (SCCRQ) packets may cause tunnel to reset after digest failure.

Conditions This symptom is observed when the SCCRQ packets are sent with an incorrect hash.

Workaround There is no workaround.

CSCtg41733 Memory leak on SIP UDP REGISTER Call Paths during fuzzing.

Symptom Certain crafted packets may cause memory leak in the device in very rare circumstances.

Conditions Cisco IOS router configured for SIP processing.

Workaround Disable SIP if it is not needed.

CSCti79442 Mismatched RTP payload type causes one way audio.

Symptom One way voice

Conditions Echo cancellation is enabled in AS5400 MGCP controlled by PGW, SIP to PSTN call. The RTP RX/TX counters will increment with **show call active voice brief**.

Workaround Explicitly define the MGCP codec type in IOS:
mgcp codec g711ulaw packetization-period 20

CSCsz43987 IOS coredump when sending crafted packets.

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

http://www.cisco.com/warp/public/707/cisco-sa-20100922-cucm.shtml

CSCtc73759 H323 gatekeeper crashing upon receipt of specific traffic.

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

CSCtd33567 Traceback seen when receiving crafted H.323 packets.

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

CSCtd86472 NAT H.225.0 DoS Vulnerability.

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

CSCtf17624 NAT SIP: Crash at ipnat_clear_sd.

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

CSCtf72678 IOS Coredump Generated when sending crafted packets.

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

http://www.cisco.com/warp/public/707/cisco-sa-20100922-cucm.shtml

CSCtf91428 NAT H.323: router crashes in IP Input [in LL_Get].

The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Open Caveats - Cisco IOS Release 12.4(22)YB6

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(22)YB6

CSCte14603

A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

CSCta45116 Eap-fast authentication fails between router and client.

Symptom EAP-FAST authentication fails between router and client (PC or laptop running ADU).

Conditions The symptom is observed when the wireless client is running "ADUv2.x" and the router is running with Cisco IOS Release 12.4(15)T8.

Workaround Upgrade the wireless client ADU to version 3.x or 4.x.

CSCsz45567 Cisco IOS Software Crafted LDP Packet Vulnerability.

A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at Cisco Security Advisory: Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability.

`CSCsq86120 Scheme CLI Option is missing after selecting Random cantact under sip-ua.`

Symptom Not able to use "scheme" sub cli under "sip-ua" registrar CLI, if any other option is selected first.

Conditions When any option (sub-CLI) after the Registrar Server is selected.

Workaround Use the "scheme" option first, then follow it up with other options, after "registrar " under sip-ua sub-mode.

`CSCsy09250 Bus error and crash when crafted packet is sent to device.`

Skinny Client Control Protocol (SCCP) crafted messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

This advisory is posted at Cisco Security Advisory: Cisco IOS Software NAT Skinny Call Control Protocol Vulnerability.

`CSCsz45567 Cisco IOS Software Crafted LDP Packet Vulnerability.`

A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at Cisco Security Advisory: Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability.

CSCta45116 Eap-fast authentication fails between router and client.

Symptom EAP-FAST authentication fails between router and client (PC or laptop running ADU).

Conditions The symptom is observed when the wireless client is running "ADUv2.x" and the router is running with Cisco IOS Release 12.4(15)T8.

Workaround Upgrade the wireless client ADU to version 3.x or 4.x.

Open Caveats - Cisco IOS Release 12.4(22)YB5

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(22)YB5

CSCsz75186

Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-tcp.shtml.

CSCsz48680

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

Cisco has released free software updates that address these vulnerabilities. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-sip.shtml.

CSCta19962

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml.

CSCtb93855

The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml

CSCsz48614

Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-cucme.shtml.

CSCtd63474 MGCP GW ACK in G729 codec but streaming in G711.

Symptom GW is streaming with the wrong codec g711 and IP phone is expecting g729.

Workaround There is no workaround.

CSCsh70718 RIP is not sending or processing updates via the interface.

Symptom RIP is not sending or processing updates via the interface.

Conditions The issue occurs after the following commands are issued in sequence:

shut the interface -> remove ip address from the interface -> no shut --> remove the network from rip --> reconfigure the ip address on the interface --> no shut -> reconfigure the network under router rip.

Workaround There is no workaround.

CSCsm47881 "CCE match" string not seen in the debug messages.

Symptom "CCE match" string is not found in the debug messages.

Conditions This error is seen in Cisco image version 12.5(0.11).

Workaround There is no workaround.

CSCsu45780 "dsxpnm_gt96k_abort_tx_mpsc:Aborting Tx mpsc failed" error with NM-1T3/E3.

Symptom The following error message is displayed if the DSU bandwidth is configured with a value other than the default of 44210 for T3 on an NM-1T3/E3 module:

```
dsxpnm_gt96k_abort_tx_mpsc:Aborting Tx mpsc failed
```

Conditions The symptom is observed when the DSU bandwidth is changed to a value other than the default of 44210. It mostly occurs with values below 1000.

Workaround Leave the DSU bandwidth at the default of 44210.

CSCsv01474 **ip rip advertise** command lost after interface flap/clear ip route.

Symptom The **ip rip advertise** command might be lost from the interface.

Conditions This symptom occurs in any of the following three cases:

- The interface flaps.
- The **clear ip route** command is issued.
- The **no network <prefix>** command and then the **network <prefix>** command are issued for the network corresponding to the interface.

Workaround Configure the **timers basic** command under the address-family under **rip**.

CSCsv12067 "fax protocol t38" CLI displays twice in **sh run** under "dial-peer".

Symptom Configuring "fax protocol t38" under "dial-peer" displays the entry twice in **sh run**.

Conditions This issue is seen in 12.4(22.3)PI10b image.

Workaround There is no workaround.

CSCsv36769 CUBE/ GK cannot handle multiple BRQ/BCF when HD video is enabled.

Symptom When HD video is enabled through Codium conferencing bridge, Codium sends multiple BRQ/BCF, CUBE is not able to handle it and is not able to open H245 channels subsequently.

HD polycom =====CUBE/GK======Codium===HD Polycom

Workaround Do not use gatekeeper. Direct HD call across the CUBE with dial peers work.

CSCsv62323 UC520, C880, VG202, VG204, IAD2435-8FXS, and C1861 routers vulnerability.

Symptom The Fast Ethernet driver code may cause several errors. The observed symptoms of this issue include:

- Cisco Unified Communications 500 series routers (UC520) may crash with an "Unexpected exception to CPU" error.
- Cisco 1861 router may fail to establish L2TPv3 session with an error message: "%L2TP-3-ILLEGAL: _____:_____: ERROR: unsupported transport protocol; defaulting to UDP if possible"

Conditions The symptoms are observed with the following hardware platforms: UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS and Cisco 1861 routers. In addition, the following conditions exist:

- The UC520 must be configured with a BVI interface. For example:

  interface BVI1 ip address 192.168.0.1 255.255.255.0
- The Cisco 1861 router is configured with L2TPv3. For example:

  pseudowire-class l2tpv3 encapsulation l2tpv3 ip local interface Loopback0 ! interface Loopback0 ip address 192.168.10.1 255.255.255.255 ! interface FastEthernet0 no ip address xconnect 192.168.0.1 1 pw-class l2tpv3

Workaround There is no workaround.

Further Problem Description: The issue is caused by an underlying driver vulnerability that exists in the UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS, and Cisco 1861 routers. No other model of Cisco routers or switches are known to be affected by this issue. The symptoms can be triggered with specific TCP sequences.

CSCsw67252 T.38 re-invite using rtp-nte when t38 and rtp-nte are both enabled.

Symptom When RTP-NTE and T.38 are both enabled, the re-invite for T.38 incorrectly includes Session Description Protocol (SDP) with RTP-NTE.

Conditions Occurs when both RTP-NTE and T.38 are enabled.

Workaround There is no workaround.

CSCsx20984 Router reloads with bus error and no stack trace.

Symptom Router reloads with a bus error and no tracebacks.

Conditions Unknown.

Workaround There is no workaround.

CSCsx97093 AAA Fails to parse RADIUS callback string ending in =.

Symptom When trying to parse a callback string attribute in an ACCESS-ACCEPT, which has no callback value, RADIUS/DECODE fails:

```
*Feb 24 16:04:22.252: RADIUS: Received from id 1645/68 10.48.88.121:19645,
Access-Accept, len 52 *Feb 24 16:04:22.252: RADIUS: authenticator 49 7C 52 33 F8
BF 21 49 - 6C EF EC 2C 6D 09 92 BD *Feb 24 16:04:22.252: RADIUS: Vendor, Cisco
[26] 32 *Feb 24 16:04:22.252: RADIUS: Cisco AVpair [1] 26
"lcp:callback-dialstring=" *Feb 24 16:04:22.252: RADIUS(00000000): Received from
id 1645/68 *Feb 24 16:04:22.252: RADIUS/DECODE: convert VSA string; FAIL *Feb 24
16:04:22.252: RADIUS/DECODE: cisco VSA type 1; FAIL *Feb 24 16:04:22.252:
RADIUS/DECODE: VSA; FAIL *Feb 24 16:04:22.252: RADIUS/DECODE: decoder; FAIL *Feb
24 16:04:22.252: RADIUS/DECODE: attribute Vendor-Specific; FAIL *Feb 24
16:04:22.252: RADIUS/DECODE: parse response op decode; FAIL
```

Conditions Any of the following callbacks fail parsing when configured with NULL value: "arap:callback-dialstring=" "slip:callback-dialstring=" "shell:callback-dialstring=" "lcp:callback-dialstring="

Workaround There is no workaround.

CSCsz69033 SIP DO-DO Video calls are failing on CUBE.

See CSCtc82324.

CSCta22394 **ip rip initial-delay** doesnt work as expected.

Symptom When RIP is configured between Cisco and third party devices, the RIP process ignores delay and keeps sending messages out even though the **ip rip initial-delay xx** command is configured.

Conditions When using **ip rip initial-delay xx** as a way to achieve interoperability between third party product and Cisco devices while using RIP authentication.

Workaround Remove authentication.

CSCta26716 Fix stdarg.h/stddef.h.

CSCta63555 CME crash after submitting SNR number change menu from EM phone.

Symptom Router crashes when running with Cisco IOS Release 12.4(24)T or later.

Conditions The symptom is observed if the SNR number change menu is selected from an extension mobility phone. The router crashes after submitting the change.

Workaround Configure an SNR under the user-profile or logout-profile with which the extension mobility phone is provisioned.

CSCtb16522 DDNS HTTP packet has password limited to 15 characters.

Symptom DDNS password is limited to 15 characters when using HTTP.

Conditions Issue is observed on Cisco 880 platform running 12.4(22)YB3.

Workaround Use shorter password.

CSCtb34444 RTP to SRTP call fails via CUBE.

Symptom Non-secure to secure call fails via CUBE.

Conditions When a call is placed between non-secure to secure leg, CUBE fails to invoke secure transcoder configured on the box.

Workaround There is no workaround.

CSCtb66963 Comma in CC-Diversion/Diversion/CC-Redirect Header causes 400 Bad Request

Symptom SIP call from a call forwarded phone to a Cisco IOS VoIP gateway is rejected when INVITE contains a comma in the Diversion Header.

Conditions Example on an inbound SIP invite that contains a Diversion field such as this:

```
---- Received: INVITE sip:15551111111@10.1.134.116:5070 SIP/2.0 Via: SIP/2.0/UDP
172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 Remote-Party-ID:
<sip:5555555555@172.27.128.130>;party=calling;screen=yes;privacy=off From:
<sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9-3843c1b221cc-53184879? To:
<sip:15551111111@10.1.134.116> Date: Sat, 29 Aug 2009 08:06:56 GMT Call-ID:
e9edd580-a981e1a0-109-82801bac@172.27.128.130 Supported: timer,replaces Min-SE: 1800
User-Agent: Cisco-CCM5.1 Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE,
REFER, SUBSCRIBE, NOTIFY CSeq: 101 INVITE Contact: <sip:5555555555@172.27.128.130:5070>
```

```
Expires: 180 Allow-Events: presence Session-Expires: 1800 Diversion: "Smith, John"
<sip:87007@172.27.128.130>;reason=unconditional;privacy=off;screen=no Max-Forwards: 7
Content-Type: application/sdp Content-Length: 214 ----
```

The IOS gateway responds back with a:

```
---- Sent: SIP/2.0 400 Bad Request - 'Malformed CC-Diversion/Diversion/CC-Redirect Header'
Reason: Q.850;cause=100 From:
<sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9-3843c1b221cc-53184879
Content-Length: 0 To: <sip:15551111111@10.1.134.116>;tag=B8C0430-6C Call-ID:
e9edd580-a981e1a0-109-82801bac@172.27.128.130 Via: SIP/2.0/UDP
172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 CSeq: 101 INVITE ----
```

Workaround Modify the diverting name associated with the redirecting device so that it does not contain a comma.

CSCtb70547 SIP GW signaling over TLS transport is unavailable.

Symptom The "Cisco IOS SIP Gateway Signaling Support Over TLS Transport" feature introduced in IOS 12.4(6)T is not configurable on the VG224 or IAD2430 platforms.

Conditions This behaviour is observed on the VG224 and IAD2430 voice platforms in any release of IOS which supports the "Cisco IOS SIP Gateway Signaling Support Over TLS Transport" feature. Specifically IOS 12.4(6)T and later the 12.4T release train is affected, as are any IOS trains derived from 12.4T.

The affected feature sets are:

VG224: IP SUBSET/IPSEC 64 BIT/VOICE (vg224-i6k9s-mz) IAD2430: IP SUBSET/IPSEC 64BIT/FW/VOICE (c2430-i6k9o3s-mz)

The IAD2431 and IAD2432 are not affected by this issue, and use the following IOS feature set:

IAD2431/IAD2432: IP PLUS/IPSEC 64BIT/FW/VOICE (c2430-ik9o3s-mz)

Workaround Use an unaffected platform.

CSCtb74251 On hook dialing did not work on 7911 SCCP Phone.

Symptom

1. Shutdown CUCM service SCCP Phone 7911 registered with SRST
2. Keep the phone on the hook
3. Press "New Call" softkey, nothing happens.

Workaround There is no workaround.

CSCtb78700 % Line 4 not available for clearing [OK].

CSCtc42058 SIP headers generated by TclIVR are not included in outgoing SIP INVITE.

Symptom SIP header AVList pairs passed from the Tcl/IVR layer are ignored in SIP-SIP configuration.

Conditions SIP-SIP configuration with header-passing enabled.

Workaround There is no workaround.

CSCtc76889 Fix for CSCsv36769 not integrated in 12.4(22)T1 and 12.4(22)YB4 IOS.

Symptom CUBE/GK is not able to handle multiple BRQ/BCF requests/responses in 12.4(22)T1 and 12.4(22)YB4 IOS. The fix for CSCsv36769 was supposed to be integrated in these releases but this integration with the above IOS did not take place.

Conditions Video over CUBE/GK, CUBE/GK is not able to handle multiple BRQ/BCF request/responses resulting in one-way video.

Workaround Do not use gatekeeper. Direct HD call across the CUBE with dial peers work.

CSCtc80306 CME system message disappears from 7940 7960 display.

Symptom A Cisco 7940 or a 7960 IP Phone registered to a Cisco Unified Callmanager Express system may lose its "system message" (default is "Your current options") intermittently for a period of 5 seconds to 45 seconds.

Conditions The conditions are:

1. Problem phone (A) is programmed with a monitor line appearance on phone.
2. Source phone (B) of monitored line starts a call.
3. Phone A monitor button correctly displays that phone B is on call.
4. Source phone B ends call.
5. Phone A loses system message for a period of 5 seconds to 45 seconds.

Workaround The problem only affects phone models 7940 and 7960 at this time.

CSCtd03857 Called Name (Forward To) incorrect for call to CFA phone, at alerting.

Symptom Called Name (Forward to) is incorrect for call to CFA phone, at alerting stage of call.

Conditions In the following scenario the calling IP phone (A) displays the wrong called name (forward to) at the alerting stage. The Phone (A) displays its own name as the Forward to name. After the call is connected, the correct name (C) is shown.

A--Calls-->B--CFA-->C

Workaround There is no workaround.

CSCtd33994 Consult Transfer Scenario is Failing.

Symptom Consult transfer fails across SIP trunk.

Conditions The triggered invite does not include a replaces header.

Workaround Disable refer on the SIP trunk.

CSCtd48917 http_get on filesystem fails for files greater than 2048 bytes.

Open Caveats - Cisco IOS Release 12.4(22)YB4

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(22)YB4

CSCsz89904

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

Cisco has released free software updates that address these vulnerabilities. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-sip.shtml.

CSCsz49741

Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-cucme.shtml.

CSCsu70214

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

CSCsv48603

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

CSCsx07114

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

CSCsu50252

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

CSCsy54122

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

CSCsy15227

Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml

CSCsz38104

The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml.

CSCsr18691

Cisco IOS devices that are configured with Cisco IOS Zone-Based Policy Firewall Session Initiation Protocol (SIP) inspection are vulnerable to denial of service (DoS) attacks when processing a specific SIP transit packet. Exploitation of the vulnerability could result in a reload of the affected device.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available within the workarounds section of the posted advisory.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090923-ios-fw.shtml

CSCsx70889

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

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

CSCsq01966 FAX with G711 RE-INVITE fails.

Symptom Fax call initiated as T.38 and attempts to fallback G711 fails.

Conditions Call established is G729, SIP trunk RE-INVITE's with T.38 and CUBE rejects due to it's configured settings (fax passthrough G711), SIP Re-INVITE's with G711 call fails.

Note: if CUBE is configured for T.38 call fax is successful.

CSCsr41631 SSLVPN does not interoperate with IP features - FW, NAT, and PBR.

Symptom Any Connect client connecting to a Cisco ISR router that is running Cisco IOS Release 12.4(20)T with hardware encryption and CEF enabled, is unable to reach the inside interface IP address but can communicate with devices behind the router.

Conditions This symptom is observed with Cisco IOS Release 12.4(20)T with hardware encryption and CEF enabled.

Workaround Disable CEF globally and/or disable hardware encryption.

CSCsr88058 Multicast stops when ingress netflow is configured.

Symptom Multicast stops flowing through the dot1q enabled interfaces on the router. This is also seen for non dot1q interfaces with 12.4(20)T.

Conditions A 3800 series router is running 12.4(20)T spservicek9 image only and you have dot1q subinterfaces configured with multicast traffic coming in one interface and exiting the other interface. When you enable ingress netflow on the receive interface of the multicast traffic, the interface will stop processing multicast traffic.

This is also seen in 12.4(20)T Advanced IP Services feature set when the incoming interface for (S,G) has IP flow ingress configured on it.

Workaround

1. Remove ingress netfow from the multicast ingress interface.
2. Switch IOS to a different 12.4(20)T feature set, other then spservicek9, that fits the functionality of your configuration.

CSCsu00313 SIP SRTP call flow fails through IP-IP GW.

Symptom SRTP call fails through the IP-IP gateway with SIP end points.

Conditions SRTP call may fail with SIP trunk in between two CUCMs that are connected through IP-IP gateway.

Workaround There is no workaround.

CSCsu42156 **Call threshold** command behaves differently when GK is used.

Symptom The **call threshold** command behaves differently when GK is used. It allows more calls then expected.

Conditions Occurs on a router running Cisco IOS Release 12.4(21.14)T1.

Workaround There is no workaround.

- CSCsu48354 CUBE - CVP: Needs Record-Route turned on in CUPS for transfer to agent DN.

Symptom Agent goes reserve, caller hears ringback, and does not get connected to agent.

Conditions CVP 4.0.2 CUBE 12.4.15T05 CUPS 1.0.3 CCM5.1.3 ICM 7.2.2

Record-Route in CUPS is turned off.

Workaround Turn on Record-Route in CUPS.

CSCsu78975 Crash seen @adj_switch_ipv4_generic_les on 38xx router.

Symptom Crash seen @adj_switch_ipv4_generic_les on 38xx router.

Conditions This issue is seen while unconfiguring/on issuing CLI **no ip route** *10.2.82.0 255.255.255.0 vlan1*.

Workaround There is no workaround.

CSCsv36769 CUBE/GK cannot handle multiple BRQ/BCF when HD video is enabled.

Symptom When HD video is enabled through Codium conferencing bridge, Codium sends multiple BRQ/BCF, the CUBE is not able to handle it and subsequently is not able to open H245 channels.

Conditions HD polycom =====CUBE/GK======Codium===HD Polycom

Workaround Do not use gatekeeper. Direct HD call across the CUBE with dial peers works.

CSCsv47202 CUBE up-speed to G711 fax fails when codec filtering is applied.

Symptom Codec filtering is configured on the CUBE for SIP-SIP call flows. After the initial call is established with G729 codec and fax tone is detected, upspeed to G711 codec does not work and the fax call fails.

Conditions Codec filtering (voice class codec) is configured on CUBE and initial G729 SIP-SIP call upspeeds to G711 due to fax tone detection.

Workaround Use separate G711 dialpeers to fax DID numbers to avoid upspeed. If deploying with CUCM, place the fax numbers in G711 region and have a separate G711 trunk to CUBE for fax calls.

CSCsv52332 Deleting FW and then NAT causes UC500 to crash.

Symptom IOS router may reload when deleting QoS policy from a router with NAT configured on the same interface and in the same direction.

Conditions A router is configured with both QoS and NAT in the same direction on an interface.

Workaround Delete IP NAT before QoS policy.

CSCsw51214 Basic SRTP call fails through IPIPGW.

Symptom A Secure Real-Time Transfer Protocol (SRTP) call might fail through a Cisco Multiservice IP-to-IP Gateway (IPIPGW).

Conditions The symptom is observed when an SRTP call is made between two Cisco Unified CallManager (CCM) with an IPIPGW in between.

Workaround There is no workaround.

CSCsw64933 "&" amp sign in VXML script cause TTS to stop working.

Symptom VXML gateway might stop providing audio prompts to caller.

Conditions When TTS text contains "&" which escapes as "&", the XML parser converts it to "&". VXML interpreter does not escape it when sending the TTS to the server. This causes TTS generates a parse error.

Workaround Remove the "&" in the VXML script.

CSCsw65430 Basic call is failing for G726 codec for DO-->SS.

Symptom Calls fail when G726 codec is used in SS-DO-SS call scenario.

Conditions Call fails when G726 codec is used.

Workaround There is no workaround.

CSCsw87515 No media in Alert Transfer with two CUBEs.

Symptom Consult Transfer/Alert Transfer fails.

Conditions Call transfer fails in both Consult Transfer/Alert Transfer scenarios.

Workaround There is no workaround.

CSCsx55878 PVC goes to inactive status when vbr-nrt traffic class is applied in an 878.

Symptom In an 878 router, the PVC remains in inactive state when VBR-NRT is applied for that particular PVC. The IOS version where this is seen is 12.4(22)T.

Conditions VBR-NRT is configured as a class of service under a PVC. The issue is not seen with IOS 12.4(15)T5.

Workaround Use CBR instead of VBR-NRT class of service. With IOS 12.4(15)T5, this issue is not seen.

CSCsx72423 After upgrade, mgcp_parse_v110_asynch_parms is seen in the log.

Symptom Logging buffer is overloaded with mgcp_parse_v110_asynch_parms messages. No calls are failed.

Conditions This issue is seen in AS5400XM with IOS 12.4(22)T.

Workaround There is no workaround.

CSCsy15926 Unsupported features should be removed from the 860 and 880 series.

Symptom Some unsupported features might be available for configuration on the 860 and 880 platforms. See the product datasheets for a list of supported features on the 860 and 880 platforms.

860 datasheet:
http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_461543.html

880 datasheet:
http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542.html

Workaround There is no workaround.

CSCsy29940 Unable to inspect any protocol in self zone.

Symptom Unable to configure inspect for any protocol in self zone.

Conditions When class-map is configured with match protocol and tries to attach to self zone pair.

Workaround This issue is not seen when match access-group is used.

CSCsy84474 OLC-ACK is not forwarded when Connect is received between OLC and OLC-ACK.

Symptom In an H323 IP-to-IP Gateway (IPIPGW), during call setup when the OLC-ACK is received after the connect message, the call is not completed and the return OLC-ACK is not forwarded by the IPIPGW. The issue is sporadic and does not occur all the time.

Conditions This has been observed on an IPIPGW running Cisco IOS Release 12.4(20)T1-ES, having an H323 on both sides of the gateway. This occurs only when the connect message is received before OLC-ACK exchange between the parties is complete.

Workaround There is no workaround.

CSCsz17680 G/W Crashes when an in-dialog Refer is sent in a 3PCC OOD-R CallFlow.

Symptom Crash is seen in 3PCC OOD-R CallFlow when an in-dialog Refer is sent.

Conditions Application misbehaves and sends an in-dialog Refer in a 3PCC OOD-R CallFlow.

Workaround There is no workaround.

CSCsz24692 c881 and c89x Wan FE stops pinging when Tx Ring becomes full.

Symptom The FE wan might stop transmission.

Conditions This happens when the interface is configured with ‘speed 10’, ‘duplex half’ and you have performed **shut**, **no shut** many times.

Workaround Reset the interface by issuing **clear int ...** or **shut** followed by **no shut**.

Further Problem Description: The transmission (tx) stops since the tx buffer descriptor (bd) ring is full. When it occurs, **show controller ...** will show that the tx bd ring has 64 used entries and there are no free entries for new frames.

CSCsz29066 BGP is not supported with the 880 Advanced Security Feature set.

Symptom BGP is not supported by the Cisco 880 Advanced Security Feature set as per the datasheet at http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542.html

This feature is configurable using the Advanced Security Feature set.

Conditions BGP configuration.

Workaround There is no workaround.

CSCsz33415 Display-logout message stays on the phone after removing it from the config.

Symptom Display-logout messages stay on the screen of the phone after removing it from the configuration of the hunt group (ephone-hunt).

Conditions The issue occurs when the display-logout messages are removed from the configuration when no phone is logged into the hunt-group.

Workaround Restart the router after the configuration change.

Further Problem Description: Even though the messages stay on the screen, the hunt group works fine and phones are able to log in and log out of the hunt-group. Also, this issue is not seen when the display-logout message is removed when the phones are still logged into the hunt-group.

CSCsz45855 CUBE not responding to reINVITES received while call transfer is in progress.

Symptom Cisco Unified Border Element (CUBE) ignores reINVITEs from Cisco Customer Voice Portal (CVP).

Conditions While call transfer is in progress and CUBE is waiting for NOTIFY (with 200 or any final response code) after receiving NOTIFY (with 100), it receives INVITE.

Workaround There is no workaround.

CSCsz45898 SIP-SIP CUBE does not forward 200ok for session refresh.

Symptom SIP Provider -[sip]- CUBE -[sip]- CUCM

CUBE does not respond to the second reINVITE to refresh the session causing the session refresher to timeout and drop the call.

Conditions Media flow around configured on CUBE - CUBE running any IOS beginning with 12.4(22)T - INVITE method to refresh the session.

Workaround Configure media flow through on CUBE. If that is not possible, downgrade to any IOS before 12.4(22)T when media flow around is configured. For example, 12.4(20)T, 12.4(15)T, etc.

CSCsz48286 Crash due to memory block overrun of 1 byte.

Symptom A router configured for VOIP might crash due to memory corruption when performing a consultation transfer. A call transfer is considered consultative when the transferring parties either connect the caller to a ringing phone (ringback heard) or speak with the third party before connecting the caller to the third party.

Conditions The crash occurs when trying to attempt a consultation transfer outside of the router to a number with more than 23 digits.

Workaround There is no workaround.

Further Problem Description: The space in memory is allocated incorrectly. When a large number is stored, memory corruption occurs and the device crashes.

CSCsz58813 UC500: %PQII_PRO_FE-4-QUEUE_FULL - IP traffic stops working.

Symptom Cisco UC500 console displays the following log(s) constantly:

%PQII_PRO_FE-4-QUEUE_FULL: Ethernet Switch Module transmit queue is full.

Phones and hosts connected to the UC can not retrieve IP addresses via DHCP.

Conditions This problem occurs shortly after a reload of the Cisco UC500 (on the CME side). This problem is observed after upgrading from Cisco IOS Release 12.4(20)T2 to Cisco IOS Release 12.4(20)T3.

Workaround There is no workaround.

CSCsz63400 Memory allocated on a CUBE leaks on receiving a REFER message.

Symptom Memory leaks are found on a CUBE when it receives a REFER message.

Conditions Once the CUBE receives a REFER message it generates an INVITE.Later the memory leaks can be found on the CUBE.

Workaround There is no workaround.

CSCsz74629 Delay in propagation of interface link state is down.

Symptom Delay in propagation of interface link state down can be observed. Link failure can be detected with huge delay once the other end of the link gets disconnected.

Conditions Problem was observed on 12.4(24)T IOS version on Cisco 1861.

Workaround There is no workaround.

CSCsz81308 c800 router hangs with 'TLB Miss exception' error on **send break**.

Symptom Using s**end break** causes router to display ‘TLB Miss exception’ error and hang indefinitely.

Conditions Occurs on a Cisco 800 router running Cisco IOS Release 12.4(24.6)T9.

Workaround There is no workaround.

CSCsz84392 UC500 does not report FRU information for certain VIC modules.

Symptom When certain VIC modules are installed in a UC500, the UC500 does not correctly report the Product (FRU) Number in the **show diag** output. If the UC500 is managed using the command line, this problem is cosmetic in nature, but if it is managed by CCA, then the VIC module is not detected.

Conditions So far, the problem has been observed with older VIC2-2BRI-NT/TE modules, with newer versions apparently being unaffected. However, it is possible the problem might be present on other VIC modules as well. All versions of UC500 software are affected.

Workaround The problem might be worked around in some cases by replacing the VIC module with a more recently manufactured unit.

CSCsz89904 CUBE crashes after codenomicon runs with Replaces header tests.

Symptom Crash after invalid Replaces header is received.

Conditions Occurs during a malicious DOS attack where attacker sends malformed headers.

Workaround Access lists, policy based control plane policing or firewalls can prevent this attack unless the attacker has spoofed a known source IP and destination port.

CSCta14362 Only one notification was sent after multiple OMA-DM sessions completed.

Symptom Only one notification is received when multiple OMA-DM sessions are completed.

Conditions Deny first NI PRL request, followed by multiple CI PRL or CI DC requests.

CSCta24094 Unsupported features should be removed from advipservice of 880 series.

Symptom Some unsupported features may be available for configuration on advipservices image of 880 platforms.

Workaround For a list of supported features on the 860 and 880 platforms, see the product datasheets.

860 datasheet:
http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_461543.html

880 datasheet:
http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542.html

CSCta30800 On issuing **clear int atm 0** Rx path goes down, but Tx path works fine.

Symptom Rx path hangs (i.e no Rx traffic) on C88x with ADSL interface.

Conditions The problem is seen in any of the following scenarios:

1. Reloading the router while pumping Rx traffic at 16Mbps (2000 packets/second with packet size 1024).
2. Issuing **clear int atm 0**.
3. Adding and removing PVC while Rx traffic is pumped.

Workaround Perform **shut / no shut** on the atm interface.

CSCsz71348 Port MIrroring Session stops working after a while.

Symptom UC500 port mirroring stops forwarding traffic to the destination port after a period of time.

Conditions This was observed on a UC520-8U-4FXO-K9 running 124-20T2 and 124-24.T.

Workaround Remove the monitor session and reconfigure it.

Open Caveats - Cisco IOS Release 12.4(22)YB3

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(22)YB3

CSCta78314 C887, C867, and C886 platforms minimum rommon version for boot up.

Symptom C887, C867, and C886 platforms require minimum rommon version 12.4(22r)YB3. Platforms shipped from manufacturing might be running with upgrade rommon with this version. If this platform is booted with read-only rommon, the unit will not function properly.

Conditions Platform booted with read-only rommon will not boot properly.

Workaround Boot these platforms using upgrade rommon.

CSCsz85550 license requested when entering card type T1 (VWIC-2/MFT1-T1/E1) uc520.

Symptom A UC500 running 12.4(22)YB1 (IOS in Early Adopter package 7.1.1) and with a T1/E1 VIC installed, will experience the following problem when trying to configure the Voice Card:

```
UC520(config)#card type t1 0 2
To  configure card type command install HWIC T1E1 license  first.
Please  use:license install <filename>
```

Workaround Upgrade the IOS to an image with the fix. To obtain an image with the fix, open a case with TAC. Support information can be found at:

http://www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html

CSCsz53057 Alignment errors seen with l2tpv3 and HWIC-3G.

Symptom The following syslogs may be seen reported by a router:

```
May  5 18:54:22: %ALIGN-3-CORRECT: Alignment correction made at 0x4093A698  read
ing 0x3D2E2AAF
```

```
May  5 18:54:22: %ALIGN-3-TRACE: -Traceback= 0x4093A698 0x4092F3A8 0x40930EE8
0x41D0821C 0x41D09228 0x41D08310 0x41D09228 0x41D09940
```

Conditions l2tp configured over a 3G WIC or HWIC.

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 12.4(22)YB2

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(22)YB2

CSCsk41593 PAK_SUBBLOCK error found when pinging with >1500-byte over cellular inter.

Symptom The following error occurs when a ping packet is sent or received:

```
PAK_SUBBLOCK_ALREADY: 2 -Process= "IP Input"
```

Conditions Occurs when large ping packets (greater than 1500 bytes) are sent to back-to-back cellular interfaces with GRE tunneling enabled.

Workaround Disable the **ip virtual-reassembly** command on the cellular interface.

CSCsl66558 Traceback occurred in the AS5400 @ ccsip_call_setup_request.

Symptom Traceback is seen in the AS5400 @ ccsip_call_setup_request.

Conditions Traceback occurred in the sip @ ccsip_call_setup_request. This is seen after making the cas(fgb)calls in the AS5400 box. This was not observed on the 12.4(17.4)T1 image.

Workaround Unknown.

CSCsm21604 Backward compatibility for codec g726r32 not working.

Symptom MGCP gateway does not allow backward compatibility with g726r32 to use static payload and the call is negotiating to doec g711ulaw.

Conditions This causes call failures when interworking with gateway which uses static payload.

Workaround Dynamic payload can be used.

CSCso59961 c3825 encounters traceback @ ipsendnet_internal.

Symptom Traceback seen when testing with ipip gateway supplementary services.

Conditions The problem happens for 12.4(15)XZ based release.

Workaround No workaround.

CSCsq44101 Policy with match protocol and pass action cannot attach to self-zone.

Symptom When applying service-policy to firewall zone-pair containing self-zone, the following error is seen:

```
%Protocol configured in class-map <class name> cannot be configured for the self zone.
Please remove the protocol and retry
```

Conditions This issue is seen if class-map in the policy-map uses match protocol and the protocol is not in the list of supported protocols for self-zone. This issue is seen even with pass action.

Workaround Change from match protocol in the class-map to use ACL to match the port instead.

CSCsu10610 Path confirmation fails after testing mgcp caller id feature.

Symptom Path confirmation may fail after testing mgcp caller id feature on gateways running with Cisco IOS version 12.4(21.13) or later.

Conditions MGCP scenarios alone.

Workaround There is no workaround.

CSCsu32069 7200 router crash after call-home config to send HTTPS request.

Symptom The router crashes when call-home tries to establish a secure HTTP connection to a server.

Conditions

- The call-home profile has a HTTP destination address pointing to a secure HTTP server.

```
Example:
destination address http
https://172.17.46.17/its/service/oddce/services/DDCEService
```

- When there is no crypto pki trustpoint to be used by the secure HTTP connection.

Workaround Configure a crypto pki trustpoint to be used by the secure HTTP connection.

CSCsu36827 CUE clock does not sync up with CME using NTP

Symptom The CUE clock does not synch up with CME using NTP.

Conditions This symptom is observed when the UC500 is configured as the NTP master.

Workaround Use an external NTP server other than the UC500.

CSCsu72242 ccm registration fails with **mgcp srtp package-capability** configured.

Symptom With the **mgcp package-capability srst-package** command configured on a CallManager/CUCM-controlled gateway, the gateway will download its configuration but will be unable to successfully register any analog or digital trunks.

Adding the command after the gateway has successfully registered to the CUCM will keep the trunks registered but all calls to the gateway will fail.

Conditions MGCP with SRTP

Workaround There is no workaround. SRTP cannot be enabled.

Further Problem Description:

When registering its capabilities with the CUCM, the MGCP sends the following:

```
09/22/2008 12:53:45.436 CCM|MGCPHandler received msg from: 192.168.1.2 200 47
X+SRTP/A: "AE, a: PCMU;PCMA;G.729;G.729a
|<CLID::StandAloneCluster><NID::192.168.1.15><CT::1,100,134,1.78><IP::192.168.1.2><
DEV::><LVL::Significant><MASK::2000> 09/22/2008 12:53:45.436 CCM|MGCPHandler PARSE
errorCode=0 for buffer: 200 47 X+SRTP/A: "AE, a: PCMU;PCMA;G.729;G.729a
```

A successful/correct syntax of the message should look like:

```
03/08/2005 11:52:54.792 CCM|MGCPHandler send msg SUCCESSFULLY to: 192.168.1.2 AUEP 50
AALN/S1/SU0/0@nw046b-1-2621xm.xyz.com MGCP 0.1 F: X+SRTP/A
|<CLID::DSL2-CM126-CM1-Cluster><NID::10.89.79.2><CT::1,100,67,1.92987><IP::192.168.
1.2><DEV::AALN/S1/SU0@nw046b-1-2621xm.xyz.com> 03/08/2005 11:52:54.792
CCM|MGCPHandler received msg from: 192.168.1.2 200 50 X+SRTP/A:
"AES_CM_128_HMAC_SHA1_32", a: PCMU;PCMA;G.729a;G.729
```

CSCsu93802 792X displaying wrong priority CME night service notify messages.

Symptom The 7921 and 7925 do not always display the `Night Service XXXX` notify message when night service is being triggered on CME. Instead `Night Service Active` may always be displayed or displayed for a long period of time.

Conditions 7921 or 7925 is registered with CME and its ephone is configured with **night-service bel**l. Night service is active in the system and a call comes into a dn which is configured with **night-service bell**.

Workaround There is no workaround.

CSCsv13562 Router crashes due to double free of ccb->call_info.origRedirectNumber.

Symptom The router crashes because of double free scenarios. While handling a 302 response, **ccb->call_info.origRedirectNumber** attempts a double free because of signaling forking. The following message appears in the crashinfo file:

```
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (2/1),process
= CCSIP_SPI_CONTROL.
```

Conditions This symptom is observed when Call Manager Express is running.

Workaround There is no workaround.

CSCsv55838 system crash after inserting bad modem.

Symptom System crash after show cellular 0 for a bad modem.

Conditions Show command for bad modem.

Workaround There is no workaround.

CSCsv76110 Attaching service policy of self-zone policy-map failure to the zone-pair.

Symptom Attaching service policy of self-zone policy-map failure to the zone-pair.

Conditions When L7 policy-map of service policy-map attached to the L4 Policy-map.

Workaround There is no workaround.

CSCsv96709 CME Join softkey does not conference on overlay DN with huntstop channel.

Symptom Unable to join 2 calls using the Join softkey - get `Can not complete conference`.

Conditions IP Phones registered to CME 7.0 - IP Phone that is doing the conferencing has 2 DNs overlaid with primary overlay DN having huntstop channel.

Workaround Do not use huntstop channel on primary DN.

CSCsv96757 steelers uut crashing while pumping traffic after config random detect.

Symptom After configuring random detect (WRED) on the ATM interface on a Cisco 888 Integrated Services router and traffic is sent through the VLAN input interface to the ATM interface, the router will display a continuous maclloc error. Additionally, the router crashes within 10-20 seconds after the traffic is stopped.

Conditions The problem is only observed on Cisco 888 Integrated Services router when WRED is enabled on the ATM interface.

Workaround Do not enable WRED on the ATM interface on the Cisco 888 Integrated Services router.

CSCsw19872 Anonymous from header translated when translation rules are used.

Symptom Translation rules wrongly translate SIP from header when it is set to Anonymous in the incoming INVITE to the CUBE.

Conditions Translation rules need to be configured to translate the calling party number.

Workaround There is no workaround.

CSCsw24542 Crash after DATACORRUPTION-1-DATAINCONSISTENCY + ALIGN-1-FATAL to isdn

Symptom A router may crash due to a bus error after displaying the following error messages:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error, %ALIGN-1-FATAL: Illegal access to a
low address < isdn function decoded>
```

Conditions The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(22)T with ISDN connections.

Workaround There is no workaround.

Further Problem Description: When copying the ISDN incoming call number for an incoming call from Layer2, the length of the call number was somehow exceeding the maximum allocated buffer size (80). PBX has pumped a Layer2 information frame with call number exceeding the maximum number length limit. It leads to memory corruption and a crash.

CSCsw49855 Ping stops working during speed/duplex testing.

Symptom IP connectivity fails for the interface following extended pings from FastEthernet interface.

show interface will indicate that the Output queue is wedged:

```
Output queue: 40/40 (size/max)
```

No more packets are switched out of the interface until the interface is cleared with the **clear interface fast<#>** command.

Conditions This has been seen on a Cisco 881 running IOS versions 12.4(20)T1 and T2. No indication at this time that this is specific to these images. The problem has been observed when the FastEthernet interface in question is set to 10/half or 100/half.

Workaround Once the problem has occurred, clear the interface with the command **clear interface fast<#>**. This problem has not yet been seen on an interface in full duplex mode. This bug will be updated as more information concerning the root cause has been gathered.

`CSCsw50802 Smart Init Fails to recognize HWICs with smart cookie.`

Symptom No extra I/O memory is allocated for some HWICs.

Conditions Occurs when HWIC is equipped with smart cookie.

Workaround Use static I/O memory configuration instead.

`CSCsw51322 Polish locale does not work on 7906.`

Symptom Polish locale doesn't work on CME.

Conditions CallManager Express 7.0(1) (but the problem exists in previous versions). It only happens on 7906. The issue occurs for all the available firmware versions.

Workaround There is no workaround.

`CSCsw75178 error.noresource event received while testing grammar scope in menu.`

Symptom Media forking request to dsp fails. The media forking feature used to send stream to ASR server will fail.

Conditions This problem is introduced by cvp based media forking feature in Pi10.

`CSCsw95072 CUCME:Blank Hlog button with Dutch locale,`

Symptom IP phone gets a blank HLOG button with Dutch locale on CallManager Express. The issue is not seen with the US locale.

Conditions IOS 12.4(22)T.

Workaround There is no workaround.

CSCsx03096 CME non-system-defined user locale config ignored after reload.

Symptom CME 7.0 configured with non-system-defined user locale via the **user-locale** command under telephony-service. The command takes effect when issued, however, it is ignored after the router is rebooted and has to be issued again.

Conditions CME 7.0 configured using Locale Installer.

Workaround Reissue the **user-locale [user-locale-tag] {[user-defined-code] country-code}** command after the router is rebooted.

Further Problem Description: The issue can be noticed after the router is reloaded and new phones are installed. They do not download the locale files. On the CME, the user locales configured can be verified via **show telephony-service** command. For example, if we have Polish locale configured in the following way:

```
telephony-service cnf-file location flash: cnf-file perphone user-locale 1 U1 load
CME-locale-pl_PL-Polish-7.0.1.1.tar
```

The correct **show telephony-service** output related to user locale should be:

```
user-locale[0] US (This is the default user locale for this box) user-locale[1] U1
language Code pl_PL user-locale[2] US user-locale[3] US user-locale[4] US
```

However, after the reboot we can see the following output:

```
user-locale[0] US (This is the default user locale for this box) user-locale[1] U1
language Code en user-locale[2] US user-locale[3] US user-locale[4] US
```

CSCsx26736 Traceback with SNMPWalk on a sysDescr MIB Object.

Symptom Traceback seen while accessing a MIB Object using SNMPwalk.

Conditions When an SNMP server public community is configured on the UUT with RW permissions and an attempt to access the sysDescr MIB Object is made, a trace back is seen.

Workaround There is no workaround.

CSCsx33278 CFA being reenabled accidentally after turning on and off night service.

Symptom Call forward all is being re-enabled on a dn after being removed.

Conditions Night service is activated and then deactivated on the dn.

Workaround There is no workaround.

CSCsx42387 Answer softkey dropping calls with CME on TNP phones with **disableSpeaker**.

Symptom Hitting the "answer" soft key drops an incoming call.

Conditions The TNP phone is configured with **disableSpeaker** set to true in its CNF vendor configuration.

Workaround There is no workaround.

CSCsx55861 C880: uut crashing while pvc comes up with **auto qos voip** configured.

Symptom C880: uut crashing while pvc comes up with **auto qos voip** configured.

Conditions WIth Auto Qos configured under ATM, when the pvc is toggled (down and up). For example, due to shut/no shut of atm interface or when cable damage is restored, the router is crashing.

Workaround If Auto qos is configured, there is no workaround.

CSCsx66982 Router crashing when multiple pvcs are configured while pumping traffic.

Symptom Router crashing when multiple pvcs are configured while pumping traffic.

Workaround There is no workaround.

CSCsx67352 %DSLSAR-3-FAILSETUPVC: Interface ATM0, Failed to setup vc 23 (Cause: VC

Symptom %DSLSAR-3-FAILSETUPVC: Interface ATM0, Failed to setup vc 23 (Cause: VC

Conditions %DSLSAR-3-FAILSETUPVC: Interface ATM0, Failed to setup vc 23 (Cause: VC setup failed)

Workaround There is no workaround.

- CSCsx94271 Call from BACD to CUE dropped due to mid call reinvite.

Symptom Drop through option used to forward call to IP Phone from B-ACD script. If the IP Phone does not answer and the call is forward to VM, the call is dropped with recover on timer expiry.

Conditions The drop is caused after the call is setup between the gateway and the CUE. The gateway sends an invite and the CUE responds with a 200 which the gateway then ACKs. After this call is setup, the gateway then sends invites with the same call-ID and incremented CSEQ number. The CUE ignores these invites so the gateway drops the call.

Workaround Increase or remove the retry-invite option under the sip-ua config on the gateway.

`CSCsy01207 CME 7975 shows only 34 speed dials for two 7915.`

Symptom The 7915 has page 1 and page 2 button so total 24 speed dials can be configured on each 7915. The first 7915 expansion module displays the 24 users, 12 on page 1 and 12 on page 2. The second 7915 expansion module displays only 10 on page 1 and none on page 2.

Conditions Load: 8.4.3 CME: 7.0.1

Workaround There is no workaround.

`CSCsy03098 Remove unnecessary start media in whisper intercom setup.`

Symptom Internally, one extra startmedia was sent out by CME.

Conditions When one way whisper intercom is established.

Workaround There is no workaround.

`CSCsy05895 IPSEC performance drops when PoE card is installed on 890.`

Symptom c890 IPSEC performance drops when PoE card is installed in the router.

Conditions Issue is there only when PoE card is installed.

Workaround Remove the PoE card.

CSCsy13055 Cannot connect to DM with speed 920kbps.

Symptom DM communication cannot be setup when configure speed is 920000.

Conditions Connected to high speed UART interface.

Workaround Lower the speed.

CSCsy14411 Chunk Memory Leak at config_voice_register_dn_sharedln.

Symptom Chunk Memory Leak is seen while unconfiguring SIP shared lines.

Conditions Observed this issue while unconfiguring shared-line in directory number voice register mode in 12.4(24.6)T image version in c3825 platform.

Workaround There is no workaround.

- CSCsy18996 TNP phones displaying `Acct` instead of `Transfer recall` in 12.4(24)T.

Symptom After a transfer recall, phones registered to CME will display `Acct` instead of `Transfer recall`.

Conditions TNP phones with firmware 8.4.2 or 8.4.3.

Workaround There is no workaround.

CSCsy20149 VG224: Voice-port goes to transient unregister under SRST mode.

Symptom STCAPP voice-port becomes transiently unregistered for approximately one minute in SRST mode.

Conditions Some STCAPP voice-port is pending switchover to SRST while active, and then when that port goes on hook and starts to switchover to SRST, the timing triggers the transiently unregistered issue on a certain port.

Workaround Wait for about a minute, and the port will automatically recover back to registered.

CSCsy22826 VG224 sending incorrect ssType in 1+ node CUCM cluster.

Symptom VG224 endpoint does not connect to callback destination, once the callback destination is idle.

Conditions Multi node cluster and VG224 endpoint is registered with node other then the first node in the cluster.

Workaround Have VG224 endpoints register with first node.

Further Problem Description:

The activation of the callback is successful. What fails is when the callback destination becomes idle again and the VG224 endpoint gets notified (ring). After the VG224 endpoint goes offhook, the system should automatically connect to the Callback destination. This does not happen and VG224 endpoint gets silence.

CSCsy28087 STCAPP Dev Cntl type is not reset after **no sccp / sccp** and switchback.

Symptom VG224 voice-ports have their device controller types stuck at SRST even after switchback to UCM.

Conditions VG224 voice-ports have switched over to SRST successfully, and then the user enters CLI commands **no sccp** and **sccp** before successful switchback to UCM.

Workaround **shut/no shut** the impacted voice-ports.

Further Problem Description:

Normally, users in troubleshooting should perform **no sccp/sccp** as well as **shut/no shut** some voice-ports to resolve some serviceability issues. However, if only **no sccp/sccp** was used but **shut/no shut** voice-ports was not, then there will be state-mismatch between stcapp and sccpapp, and can result in stcapp voice-ports' device-controller-type stuck in SRST even after having successfully switchbacked to UCM/CCM.

CSCsy28758 Hlog softkey does not work properly with EM.

Symptom HLog softkey stops working.

Conditions The symptom is observed under the following conditions:

- When logging into an EM profile where the user was logged out from the hunt group.
- This is to be done on a phone where an EM profile was previously logged in, which was also logged into the huntgroup.

Workaround Log in with the EM profile on the phone that was used to log out the huntgroup.

CSCsy32411 CME 7.x On hook transfer fails when call comes in ISDN.

Workaround Configure **transfer-pattern** with the same length of the destination number.

CSCsy43948 Crash when mtu is 64 under atm int and **ping ping <ip addr>** is issued.

Symptom When underlying exit interface of tunnel has a very low MTU, the tunnel's IP MTU gets set to a value less than IP header length. This causes a crash in fragmentation code.

Conditions Low MTU set on the physical interface (64 byte MTU).

Workaround Set physical interface MTU to a higher appropriate value.

CSCsy61209 Incorrect token found in H323 Connect message.

Symptom An IP-to-IP gateway (IPIPGW), also called CUBE, is adding an incorrect token in the H225 connect message.

Conditions The symptom is observed on an IPIPGW running Cisco IOS Release 12.4(20)T1, with talking H323 signaling protocol on both sides with security enabled.

Workaround There is no workaround.

CSCsy72468 CME 7.x: SCCP IP phones display shows ITS instead of system message.

Symptom IP phone display shows ITS instead of configured system message.

Conditions IP phone part of a huntgroup and resets or power cycled when all huntgroup members logged out.

Workaround Log into huntgroup(Hlog) and log out.

CSCsy74664 CME with SNR does not generate ringback.

Symptom No ringback heard by calling party when calling through ISDN trunk into Cisco Unified Communications Manager Express (CUCME).

Conditions IOS VoIP gateway configured as CME with ISDN trunk. When using Single Number Reach (SNR) feature on an ephone-dn (via the ephone-dn subcommand **snr**), the calling party to that phone when **snr** is active may not hear ringback indication.

Call completes without issue but the ringback may not be heard by the calling party during the alerting stage.

Workaround Only known workaround is to disable the SNR feature.

CSCsy75735 SNMP is not working with 5727 CDMA modem.

Symptom Unable to query 3g MIB with the latest PI11 image.

Conditions 5727 CDMA modem.

Workaround Use 5725 modem.

CSCsy78634 Bad double commit happens for CSCsuxxxxx in some of the throttles.

Symptom Traceback observed while configuring **rel1xx require** CLI.

Conditions Traceback can be observed after configuring **rel1xx require** CLI with a string of 49 characters.

Workaround There is no workaround.

CSCsy79893 The HLog out messages should not be overridden by system prompt.

Symptom The system prompt may be shown during Hlog out.

Conditions When an agent or all agents log out, the logout message and system message may be shown every 30 seconds.

Workaround There is no workaround.

CSCsy88059 Octo line: Second call gets dropped when the first call is put on hold.

Symptom Calls drop when answering the second call on Octo lines with the ‘Hold’ softkey.

Conditions If the calls come in a PRI or FXO interface, and a user on an active call on the Octoline puts the call on hold while there is an incoming call, it will automatically answer the incoming call. Approximately 13 seconds later the second call is dropped.

Workaround When the second call comes in, use the ‘Answer’ softkey instead of putting the first call on hold. If you want to put a call on hold while a new call is coming in, you must wait until the incoming call stops ringing.

CSCsy90652 SNR enabled ephone-dn does not provide ringback (and no voice path).

Symptom Call from CCM phone via H323 trunk to CME ephone with SNR enabled does not provide ringback to CCM phone.

Conditions SNR has to be enabled on CME ephone.

Workaround Disable SNR, then ringback will be provided to the CCM phone, but SNR won't be functional on the CME ephone.

CSCsy96789 Lost DM connection at 920K with short packet traffic (200-300pps) on GSM.

Symptom Lost DM connection a few minutes after bidirectional traffic started.

Conditions DM configured at speed 920K, Smartbit configured with 128 bytes at rate 300pps.

Workaround Use lower speed 115k.

CSCsz01236 UBR+ pvc goes inactive when the MCR value is >0kbps but <32kbps.

Symptom Failing to setup a vc with UBR+ service using MCR values less than the granularity used by an ATM driver.

Conditions For example, on a C877 ADSL router, the granularity is 32 (Kbps). The following configuration will fail to open a vc (UBR+ <PCR> <MCR>):

```
ubr+ 100 30
```

Workaround Use a minimum MCR value no less than the granularity used by the router. For example, on a C877 ADSL router with granularity of 32 (Kbps):

```
ubr+ 100 32
```

CSCsz17418 IP SLA ethernet-monitor is missing in Steelers.

Symptom Configuration command **ip sla ethernet-monitor <number>** is not supported.

Conditions In the configuration mode, this always happens.

Workaround There is no workaround.

CSCsq40088 3845 router reloads at rt_walktree_ap while unconfiguring ipv6.

Symptom A Cisco 3845 router may crash when unconfiguring IPv6 nodes.

Conditions The symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4T. The traceback is produced after configuring the **no ipv6 unicast-routing** command.

Workaround There is no workaround.

CSCsr25788 Output Drops on Gig/FE Interface when multicast traffic and NAT are enabled.

Symptom Output drops can be observed on GE/FE interface on a Cisco 2800 router.

Conditions Problem is observed when NAT is enabled while router is configured to pass multicast traffic.

Workaround There is no workaround.

CSCsw82267 entPhysicalVendorType & entPhysicalSerialNum returns wrong SNMP value.

Symptom entityMIB query for entPhysicalVendorType & entPhysicalSerialNum on c86x & c88x platforms returns wrong SNMP value.

Conditions Problem is seen across all the c86x & c88x platforms.

Workaround For correct value of entPhysicalSerialNum for Motherboard, see the `PCB Serial Number` value of **show diag** output.

CSCsw97262 NAM does not replicate packets coming from IP phone.

Symptom CLI command analysis-module not replicating packets routed from IP Phone.

Conditions IP Phone communication set up via router to FXO. Ingress interface contains **analysis-module monitoring** CLI command.

Workaround There is no workaround.

CSCsz17846 Tracebacks when pppoe-client is configured along with encap aal5ciscoppp.

Symptom Tracebacks @ pppoa_vc_up seen, when pppoe-client is configured with aal5ciscoppp virtual-template 1 encapsulation already configured.

Conditions PVC is configured with **encapsulation aal5ciscoppp virtual-template 1**. Now, when **pppoe-client dial-pool-number 1** is configured, tracebacks @ pppoa_vc_up are seen.

Workaround There is no workaround.

CSCsr62645 Software-forced reload while accessing swidbList_next.

Symptom Software-forced reload occurs on Cisco 870 router.

Conditions Encountered during extended VLAN testing.

Workaround There is no workaround.

CSCsu30540 HWIC-4SHDSL: 4Wire annex F coding 16-TCPAM link down after **shut/no shut**.

Symptom HWIC-4SHDSL: 4Wire annex F with coding 16-TCPAM link goes down after the **shut** command followed by the **no shut** command.

Conditions This symptom occurs after the 4WIRE SHDSL card with annex F coding 16-TCPAM configuration goes down after the **shut** command followed by the **no shut** command. It does not come up again. This issue is seen only with annex F coding 16-TCPAM, when annex is enabled on CPE first and then the CO side. This issue is not seen on 4WIRE SHDSL card with annex G coding 16-TCPAM.

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 12.4(22)YB1

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(22)YB1

CSCsx25880

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

CSCsy22826 VG224 sending incorrect ssType in 1+ node CUCM cluster.

Symptom VG224 endpoint does not connect to callback destination, once the callback destination is idle.

Conditions Multi node cluster and VG224 endpoint is registered with node other then the first node in the cluster.

Workaround Have VG224 endpoints registered with first node.

Further Problem Description: The activation of the callback is successful. What fails is when the callback destination becomes idle again and the VG224 endpoint gets notified (ring). After the VG224 endpoint goes offhook, the system should automatically connect to the Callback destination.This does not happen and VG224 endpoint gets silence.

CSCin93614 Wrong Packetization value is show for G723ar63 codec on IPIPGW.

CSCsm92992 nvram is not recovered if primary and backup nvram get corrupted.

Symptom Brand new NVRAM chips will not have the magic numbers written for the primary, backup, and secondary backup NVRAM. This will cause error messages when trying to read/write to the NVRAM:

Router# write erase

Erasing the nvram filesystem will remove all configuration files! Continue?

[confirm]

[OK]

Erase of nvram: complete

Router#

***Dec 17 23:08:52.319: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvramwr**

Building configuration...

[OK]

Bad configuration memory structure -- try rewriting

Bad configuration memory structure -- try rewriting

Router#

Router#

Router# wr

Bad configuration memory structure -- try rewriting

Bad configuration memory structure -- try rewriting

Building configuration...

[OK]

Bad configuration memory structure -- try rewriting

Bad configuration memory structure -- try rewriting

Router#

Workaround Load an image older than Cisco IOS Release 12.4(20)T, which will write the magic numbers. Then load an image from Cisco IOS Release 12.4(20)T or a later release.

CSCso92572 Call Transfer fails when XOR and XTO are on same side.

Symptom Call Transfer fails when XOR and XTO are on the same side.

Conditions The issue is seen for Semi-Consult and Full-Consult Transfers. It is seen only when XOR and XTO are on the same side, if they are on different sides, the call transfer goes through fine.

Workaround There is no workaround.

CSCsq83713 Memory leaks chunks at "gk process".

Symptom Memory leaks are observed in "gk process" when memory lite is disabled.

Conditions When **no memory lite** cli is configured from the global configuration mode.

Conditions Configure **memory lite** cli from the global configuration mode.

CSCsu27559 FW upgrade failed from 1.2.3.10 to 1.2.3.15.

Symptom During the firmware upgrade on 880E modem using **microcode reload** command, it is found that the modem upgrade process will stop.

Conditions Any firmware upgrade to a newer version fails.

Workaround Use the laptop based watcher to upgrade.

Further Problem Description: There are two issues associated with the failures:

- The modem boot firmware upgrade requires the host to use data channel to communicate with the modem after it is done. The current enzo only uses management channel instead of data channel.
- The driver for the modem firmware upgrade and software locking are currently tightly coupled. The locking code interferes with the firmware upgrade code during the upgrade process, thus the upgrade fails.

CSCsv01869 VPN LED is not on in ISR fixed platform when the crypto session is up.

Conditions Ensure ISAKMP is up. Observe the LED behavior.

Workaround There is no workaround.

CSCsv06649 GW sends 200OK, without waiting for PRACK for the previous 18x response.

Symptom IOS SIP Gateways send 200OK for INVITE before PRACK is received for reliable 18x response.

Conditions This happens whenever the call gets connected immediately after sending Alerting(180 response) or Progress(183 response) to the caller.

Workaround There is no workaround.

CSCsv11142 SIP-H323 hold-resume invoked from SIP leg fails.

Symptom A call is disconnected during call resume in a sip-h323 call.

Conditions This symptom is observed under the following conditions:

4. Call was held with ReInvite->ECS.
5. Received call resume ReInvite.
6. Capabilities exchanged on H323 leg.
7. Sent OLC.
8. Upon receiving OLCAck, CUBE should send ReInvite on the SIP leg; instead it sends 200OK.

Workaround There is no workaround.

CSCsv85817 CUBE: **show call active voice** displays incorrect codecbytes.

Symptom **show call active voice** command may display incorrect value for codecbytes.

Conditions This problem was observed on a H323 call using G723 codec and codec transparent configured in IPIPGW / CUBE.

Workaround There is no workaround.

CSCsw19548 DO-SS call not established in 2 ipipgw scenario.

Symptom Basic DO (Delayed Offer) to SS (Slow Start) call is not getting established in a 2 IPIP Gw scenario.

Topo-

OGW==IPIP1==IPIP2==TGW

SS==SS<->DO==DO<->SS==SS

Here the basic call is not getting established and SIP leg between IPIP1 and IPIP2 is getting into a loop with 200OK and ACK messages.

Conditions Seen when 2 IPIP Gws are connected back-to-back.

Workaround There is no workaround.

CSCsw36207 Call disconnected due to DSP battery reversal.

Symptom Outgoing of router FXO loop-start call randomly disconnected after far-end answered the call.

Conditions The far-end is able to generate reverse-battery signal when called side answered the call. Also, **supervisory disconnect** was configured to either anytone or dualtone.

Workaround Use **supervisory disconnect** signal if possible.

CSCsw36750 Basic SS-DO call is failing for 2 IPIPGWs case.

Symptom Call will be disconnected with 2 ipipgws.

Conditions In SS-DO case when initial renegotiation Re-INVITE received with only change in media direction then CUBE will not send OLC ACK

Workaround There is no workaround.

CSCsw43903 leg_remote_media_ip_address TCL infotag does not work for SIP Calls.

Symptom TCL Infotag "leg_remote_media_ip_address" may not work for SIP calls.

Workaround There is no workaround.

CSCsw75178 error.noresource Event received while testing Grammar scope in Menu.

Symptom Media forking request to dsp fails.

Conditions The media forking feature used to send stream to ASR server will fail.

Workaround This problem is introduced by cvp based media forking feature in Pi10.

CSCsw79696 Call disconnected due to DSP detects fxols_rvs_battery.

Symptom Call over the FXO loop-start cannot be established since gateway's dsp detects reverse-battery signal.

Conditions The far-end is able to generate reverse-battery signal when called side is ringing. Also, **supervisory disconnect** is configured to either anytone or dualtone.

Workaround There is no workaround.

CSCsx15347 CME as SRST needs reboot to apply G729r8 codec to ephones using template.

Symptom CME version 7.0(1) when used as SRST and configured with auto provisioning requires reboot of the router to apply codec g729r8 if mentioned in the ephone-template

Conditions Phone load - SCCP31.8-4-1S (Shipped with 7.0 CUCM)

CUCM Version - 7.0.1.11001-8

CME version 7.0(1) - 12.4(22)T

When configuring CCME as SRST mode with auto provisioning utilizing the ephone-template for soft key and codec g729r8 for the phones as following:

ephone-template 1

softkeys idle Newcall Cfwdall Pickup ConfList Join

softkeys seized Endcall Cfwdall Pickup

softkeys alerting Endcall

softkeys connected Endcall Hold Park Trnsfer Confrn ConfList Join Select

codec g729r8

Ephones register after the initial fail over to SRST and configuration is provisioned by the system, but the preferred codec used is G711ulaw instead of G729r8. However if the system is rebooted after the initial fail over, the phones register with correct codec. and "codecg729r8" shows up under the ephone in addition to ephone-template commands.

Workaround Reboot the system once the configuration (ephone and ephone-dn) is provisioned in the system.

CSCsx23053 DO--SS calls are failing with fax protocol T38.

Symptom DO--SS call involving two IPIPGWs fails.

Conditions Two IPIPGWs are involved.

Workaround Configure FS and EO.

CSCsx36327 "pass-thru content sdp" causes single connection ip address in sdp.

Symptom Telepresence calls from CTS to CTS through the CUBE connect but no video or audio is seen. If the calls are to a CTMS the call is disconnected by the CTMS with an error of "media timeout".

Show voip rtp connection shows one single ip address as the local address in the cube.

Conditions Occurs with single point to point or multipoint calls regardless of CTS model. (1000,3000, 500).

This occurs only when the CTS resides in a different subnet than the interfaces on the cube and the configuration **pass- thru content sdp** is used in the voice service voip sip menu.

This occurs in CUBE flow through mode.

Workaround If the network architecture or policy permits use the Cisco IOS **bind** command to bind media to single loopback address. This address then can be advertised to connecting networks so that media is routable to the CUBE loopback.

Further Problem Description: This issue does not affect the signalling side, just the media.

The command **pass-thru content sdp** was introduced in YB to allow flows that require a G711 codec such as music on hold. Removing this command can cause disconnects on Hold and Resume.

CSCsx47948 CME: SNR cannot be enabled on ephone-DN's with **mwi sip**.

Symptom Attempting to configure SNR on CME under an ephone-DN with **mwi sip** configured will generate the following error:

Can't configure SNR on mwi DN

As a result, SNR cannot be configured on the DN.

Conditions This is seen only on CME, using the SNR functionality first added in CME 7.1.

Workaround If using CUE, reconfigure CME/CUE for outcalling MWI method.

Directions for CME:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmevmail.html#wp1023122

Directions for CUE:

http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/rel2_3/cliadmin/ch3sys.html#wp1115186

If using third party voicemail, or using a multiple CME + Unity integration with MWI relay, there is no workaround.

CSCsx59972 intermittent call failure for xfer call to sharedline through sip trunk.

Symptom Consult transfer to SIP shared-line as a transfer-target from other CME over SIP trunk may fail.

Conditions When transferee and transferrer are at one CME, and SIP shared-line transfer target is at another CME.

Workaround There is no workaround.

CSCsx69249 SIP phones would hang after pressing hold/resume on Initiator/other-party.

Symptom When call is disconnected, shared-line resource is not released.

Conditions With cfw/busy configured, or doing park ringing pick on shared-line.

Workaround There is no workaround.

CSCsx76246 Need a new deviceID for 5x5 phones.

Symptom Phone type 501G, 502G, 504G, 508G, and 509G missing. They cannot register with CME.

Conditions When the phone is configured.

Workaround There is no workaround.

CSCsx76903 slow mem leak in mem_mgr_malloc_buf when doing REFER based transfer.

Symptom A slow memory leak occurs when a voice gateway processes a SIP REFER message that has no user portion in the Contact: and/or Referred-By: headers.

Workaround There is no workaround.

CSCsy09902 Received invalid SDP pointer from application, traceback seen.

Symptom For a call, traceback will be seen on CUBE with SDP pass-thru.

Conditions When SDP pass-thru is enabled on CUBE.

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 12.4(22)YB

CSCsw30737 NTP does not synchronize if both ntp master and ntp server configured.

Symptom NTPv4 does not synchronize with IOS 12.4(20)T and later releases. The router does not even synchronize with its own internal clock.

Conditions Need to have both ntp master and ntp server configured. If only NTP master or NTP server is configured, the router can synchronize fine with the defined time source.

Workaround If configuring only "ntp master" or "ntp server", the router will synchronize.

CSCsw88646 SCCP FXS port shared line to CCM may fail to ring or get dialtone.

Symptom With SCCP (STCAPP) FXS ports registered to CCM and assigned a shared line to SCCP IP phones, one of the following issues may occur:

- When hold/resume functionality is not configured on the SCCP gateway, and CCM's DN configuration for maximum-calls/busy trigger are set to a value of 1:, a call is placed, and an IP phone answers. The FXS phone goes off-hook and back on-hook. The IP phone then hangs up. The next call placed will not ring the FXS port. Place the call again and the FXS will ring properly again.
- When hold/resume functionality is not configured on the SCCP gateway, and CCM's DN configuration for maximum-calls/busy trigger are set to a value of >=2. Call comes into shared line. IP phone answers. While the line is in-use, the analog phone goes off-hook, then back on-hook. IP phone ends the call. From this point on the FXS port gets dead-air when going off-hook to place a call, until the stcapp process is reset with **no stcapp/stcapp**. STCAPP debugs during the issue show:

STCAPP:stcapp_get_active_call_ccb:ERROR:There is no ACTIVE call's ccb in lcb (0x645952A4) stcapp_error_handling.

Conditions The issue is seen on 12.4(20T) code, which introduces the hold/resume feature.

Workaround For the first issue there is no known workaround other than placing another call to the DN after the issue is seen, or by not having the FXS phone go offhook during active IP phone calls. For the second issue, reset the STCAPP stack as a temporary workaround, or change the max calls/busy trigger under CCM's DN configuration to be 1 for both the analog and IP phones.

Further Problem Description: Note that the second scenario is not a support solution. The max call/busy trigger should be set to 1 when not enabling hold/resume under STCAPP, which is considered a classic shared-line scenario.

To configure hold/resume on the SCCP FXS port, use:

stcapp supplementary-service

port <port>

hold-resume

```
CSCsw69730 %SIP-3-BADPAIR: Unexpected event 25 (SIPSPI_EV_CC_CALL_RESUME) shown.
```

Symptom One SIP phone originated call to another cme sccp phone, call connected, made multiple transfer back to a sccp endpoint of original cme, then observed %SIP-3-BADPAIR: Unexpected event 25 (SIPSPI_EV_CC_CALL_RESUME) shown on cme router. The call connected but audio path did not established.

Conditions The call has to originate from a SIP phone thru gateway to another cme sccp endpoint and transfer back to a sccp endpoint of original cme then xfer again to another sccp endpoint within the cme. After the cross cme call and 2 xfers, the error message shown and observed audio path failed.

Workaround There is no workaround.

Resolved Caveats - Cisco IOS Release 12.4(22)YB

- CSCsu24505

  Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml

- CSCsv04836

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

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

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

CSCsv38166

Symptom The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

Workaround There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

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

CSCsu11522

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS software that can be exploited remotely to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.

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

CSCeg87070 Crash at igmp_send_init_query.

Symptom During 7xi2b monitoring c10k crashed at igmp-process.

CSCse37273 Need Voice Translation Profile for SIP SRST Phones.

Symptom Voice Translation Profiles cannot be applied to SIP SRST phones.

Workaround There is no workaround.

CSCsg39977 Router crashes when attempt to use Dialer interface for MLP.

Symptom When dialer interfaces are used in conjunction with Multilink PPP (MLP), a router may crash because of a corrupted program counter.

Conditions This symptom is observed on a Cisco router when a dialer interface, including interfaces such as ISDN BRI and PRI interfaces, is configured to use MLP and when the queueing mode on the dialer interface is configured for Weighted Fair Queuing (WFQ). Note that WFQ is the default for some types of dialer interfaces.

Workaround There is no workaround.

CSCsh51297 No voice path after connected if CME receives 183 with sdp and then 180.

CSCsj14623 SIP Phones configured with DNs with"+" sign will not failover to SRST.

Symptom SIP phone cannot be registered if number configured by leading '+' sign.

Workaround There is no workaround.

CSCsk52143 police cir percent uses incorrect baseline bandwidth.

Conditions The symptoms are observed on a Cisco Catalyst 6509, a WS-SUP32-GE- 3B, a Cisco 7600-SIP-400, a SPA-1XOC12-POS, a Cisco 7600-SSC-400 and a SPA- IPSEC-2G using a hierarchical policy with multiple parent shapers in user- defined classes and child policies with queuing and policing actions.

Workaround Remove "police cir percent" from child queuing policy "cbwfq- sip".

Alternate Workaround: Use a different child-policy (with the same configuration). Example:

Define a second policy-map, say "cbwfq-sip1", with the same configuration as "cbwfq-sip" and change the cbwfq-ip as below:

```
policy-map cbwfq-ip
  class tunnel13601
    shape average 80000000
   service-policy cbwfq-sip
  class tunnel13603
    shape average 20000000
   service-policy cbwfq-sip1
```

(shows a different child-policy with the same configuration as "cbwfq-sip").

CSCso24954 Implement correct restrictions for queuing features with the move to HQF.

Symptom A policy with unsupported queuing features is allowed to attach to sessions. It may cause potential issues that require a reload to recover.

Workaround There is no workaround.

CSCso44189 SCCP (stcapp) fxs port on CME with station-id configured may hang.

Symptom A Cisco IOS VoIP gateway configured as a Cisco Unified Communications Manager Express (CME) with SCCP (stcapp) controlled FXS ports may intermittently be getting into a state where further calls fail through the FXS voice port.

Conditions This can occur when **<CmdBold>station-id number<noCmdBold>** is configured under the FXS voice-port and the value specified in this command matches the number defined for the configured ephone-dn. A port in this state will show a VTSP state of S_WAIT_RELEASE in the output of **<CmdBold>show voice call summary<noCmdBold>** though no active call is present and the phone on the FXS port is onhook. Further calls attempted through this port once in this state will result in the following error messages being displayed:

Jan 8 18:21:17.969: TDM: guido_port_dsp_connect: vic connect failed!

Jan 8 18:21:17.969: %FLEXDSPRM-3-TDM_CONNECT: failed to connect voice-port (1/1/3) to

dsp_channel(1/0/1)guido_disconnect_local_local, slot=1, connection 5/0 to 3/17 is not in use

guido_disconnect_local_local, slot=1, connection 3/17 to 5/0 is not in use

guido_disconnect_local_local, slot=1, connection 5/0 to 3/17 is not in use

guido_disconnect_local_local, slot=1, connection 3/17 to 5/0 is not in use

Workaround Once in this state, the router will need to be reloaded to recover. To prevent a port from getting into this state, remove the **<CmdBold>station-id number<noCmdBold>** command from the voice-port. The use of this command for stcapp controlled FXS ports does not seem to provide any benefit but can lead to the port getting into this hung state.

CSCsq42799 Only 1.5MB to 2MB downstream, when using two PA-MC-2T3-EC cards (MLPPP).

Symptom Downstream line rates of 98% or more are only being observed when using the new PA in "hardware enabled mode", meaning the MLPPP member links are on the same PA. However, when the "software mode"is used, meaning when the two member links (2 T1s) are across two different PSs, then the downstream line rate drops down to 2 Megs the most.

Workaround There is no workaround.

CSCsq73501 session and ACLs are not able to create while testing with DACL.

Symptom Unable to create sessions and ACLs.

Conditions The symptom is observed when testing with DACL.

Workaround There is no workaround.

CSCsq92019 SCCP conference controller is not working.

Symptom SCCP phone can't act as conferencing controller.

Conditions This is specific to ATT test setup where there are NAT back-to-back. NAT segmented code synchronization fails when NAT is back-to-back.

Workaround The problem doesn't exists if there is no back-to-back NAT setup.

CSCsr84713 error message whenever **show crypto session detail** issued.

Symptom Trace back is shown when **show crypto session** is issued.

Workaround Use commands **show crypto isakmp sa** and **show crypto ipsec sa.**

CSCsr94511 %SYS-6-STACKLOW: Stack for process Call Manager Application Manager.

Symptom Crash with the following message:

%SYS-6-STACKLOW: Stack for process Call Manager Application Manager running low, 0/9000

Workaround There is no workaround.

CSCsu02176 Router reloads on switching off one of the redundant power supplies.

Symptom A router reloads continuously on switching off one of the redundant power supplies.

Workaround There is no workaround.

CSCsu20411 Router is getting crashed while unconfiguring source template test.

Symptom Router may crash while unconfiguring "source template test" in interface configuration mode.

Conditions The symptom is observed with a router is loaded with Cisco IOS Release 12.4(22)T.

Workaround There is no workaround.

CSCsu24505 Intermittent crash when NTP Service is configured.

Symptom Router may crash and reload intermittently with TLB (load or instruction fetch) exception.

Conditions When a device is configured to support NTP, and running Cisco IOS versions 12.4(15)XZ, 12.4(15)XZ1, 12.4(20)T, 12.4(20)T1, 12.4(20)YA, 12.4(20)YA1, 12.4(22)MD, or 12.4(22)T it may crash because of this Cisco Bug ID.

Workaround The workaround is to temporarily remove the NTP servers from the config with:

no ntp server x.y.z.w

no ntp peer a.b.c.d

Further Problem Description: Upgrade to a version indicated in Cisco Bug ID CSCsv75948 in the Cisco bug toolkit as "fixed in". Cisco bug ID CSCsv75948 is required for a full fix.

CSCsu31042 Memory leak at pppoe_client_int_cmd.

Symptom A small memory leak may occur.

Conditions This symptom is observed when a PPPoE client or a PPPoA client is configured.

Workaround There is no workaround.

CSCsu32154 MGCP controlled fxs port intermittently gets into unusable state.

Symptom Calls through an MGCP-controlled FXS may fail to complete. The user will hear fast-busy signal when attempting to make inbound or outbound calls from or to that port. Outbound calls to the port in this state may return a 400 error "Previous message in-progress" in response to the CRCX.

Conditions The symptom is observed under rare conditions with an MGCP-controlled FXS port on a Cisco IOS Voice over IP (VoIP) gateway. To verify that a port is in this state, compare the output of <CmdBold>show mgcp connection<noCmdBold> to the output of <CmdBold>show voice call summary<noCmdBold>. If a call appears with the mgcp show command output for a port but that port appears idle (FXLS_ONHOOK) in the voice call output, this would indicate the problem being seen. To verify that a port is in this state, compare the output of **<CmdBold>show mgcp connection<noCmdBold>** to the output of **<CmdBold>show voice call summary<noCmdBold>**. If a call appears with the mgcp show command output for a port but that port appears idle (FXLS_ONHOOK) in the voice call output, this would indicate the problem being seen.

Workaround Reload the gateway to recover a port once it is in this state. Attempting to restart the MGCP service on the gateway by removing and adding the **<CmdBold>mgcp<noCmdBold>** command in the configuration has been shown at times to be ineffective once in this state.

Alternate Workaround: Use of H323/SIP signaling instead of MGCP will prevent ports from getting into this state.

Further Problem Description: Changes applied through CSCsq97697 have been found to greatly reduce the instances of this issue from occurring. If using H323/SIP instead of MGCP is not an option, it is recommended to use a Cisco IOS Release that contains the changes in CSCsq97697 (for example, Cisco IOS Release 12.4(15)T7).

The changes applied to CSCsu32154 introduce a new MGCP CLI command which is not enabled by default. If upgrading to obtain a fix for this issue, configure **<CmdBold>mgcp disconnect-delay<noCmdBold>**.

CSCsu33399 HWIC-4SHDSL:4Wire annex F/G with coding 16/32 TCPAM link on CO side down.

Symptom HWIC-4SHDSL:4Wire annex F/G with coding 16/32 TCPAM link on central office (CO) side is going down.

Conditions 4-WIRE SHDSL card with F/G annex-coding 16/32 TCPAM link on CO side is going down. CO link goes down immediately when either F/G annex is configured and never comes up. But the link on the CPE side will come up.

Issue is seen with F/G annex; the issue is not seen with A/B annex.

CO side link goes down, but the CPE comes up.

Workaround There is no workaround.

CSCsu46871 Unable to attach policy to VT with bandwidth configured in class-default.

Symptom Unable to attach service policy to VT when bandwidth is configured in class default.

Conditions Occurs when DLFI over ATM is configured while trying to attach service policy to VT when bandwidth is configured in class default.

Workaround Configure bandwidth in user defined class and attach to VT.

CSCsu49132 Router getting crashed @ rt_walktree_ap while unconguring ipv6.

Symptom A router may crash when unconfiguring IPv6.

Conditions This symptom is observed on a router that is running Cisco IOS Release 12.4T.

Workaround There is no workaround.

CSCsu51668 Box Crash- Reattach Fr Map-class/access Time-slot-hqf_centralized_pak_de.

Symptom A router may crash when reattaching a map-class or accessing the time-slots in controller mode or a router may crash when doing an OIR or flapping the peer interface.

Conditions The symptoms are observed on a Cisco 7200 series router that is configured for HQF and FRF.12.

Workaround There is no workaround.

CSCsu56748 Spurious memory seen @ ipflow_drop_punt_input_feature.

Symptom Spurious memory seen in unit test while pinging from generator to reflector.

Conditions Occurs while the ping passes through router after applying the crypto map. If the crypto map is not configured then the spurious memory will not be seen.

Workaround There is no workaround.

CSCsu56806 HSRPv6 configuration reappears after deleting/configuring SVI.

Symptom If HSRP IPv6 is configure on a vlan interface, and the vlan interface is deleted, then the HSRP IPv6 config will reappear on the vlan if the vlan is later recreated. Once this occurs there is no way to remove the HSRP config.

Workaround Problem can be avoided by removing HSRP config before deleting the vlan.

CSCsu62921 %SYS-2-BADSHARE tracebacks and traffic fails with xDSL.

Symptom %SYS-2-BADSHARE tracebacks are reported. Eventually the router will stop passing all traffic over the interface.

Conditions Occurs when sending traffic over xDSL interfaces that have QoS configured.

Workaround Remove the service-policy from the xDSL interface.

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

Symptom Router may incorrectly drop non TCP traffic. TFTP and EIGRP traffic can be impacted as seen in CSCsv89579.

Conditions Occurs when the **<CmdBold>ip tcp adjust-mss<NoCmdBold>** command is configured on the device.

Workaround Disable **<CmdBold>ip tcp adjust-mss<NoCmdBold>** on all interfaces. Note that this may cause higher CPU due to fragmentation and reassembly in certain tunnel environments where the command is intended to be used.

CSCsu64851 ILBC codec enabled FPT call is failing.

Symptom ILBC codec enabled Fax passthrough and modem passthrough call is failing.

Conditions I have observed this issue in 12.4(21.14)T2 image.

Workaround There is no workaround.

CSCsu67461 Router crashes when "show track brief" entered.

Symptom Router may crash when **show tracking brief** is entered, if one or more tracking objects have been created using the Hot Standby Routing Protocol (HSRP) cli, such as **<CmdBold>standby 1 track Ethernet1/0<noCmdBold>**.

Conditions This does not occur if all tracking objects use the new **<CmdBold>track <noCmdBold>** command as follows:

<CmdBold>track 1 interface Ethernet1/0 line-protocol<noCmdBold>

interface Ethernet 0/0

standby 1 track 1

Workaround Use **<CmdBold>show tracking<noCmdBold>** instead, or configure tracking with the new command.

CSCsu72026 OER MC reports max report limit reach when request all exit links report.

Symptom OER master controller reports an error 22 (OER_API_MAX_REPORT_LIMIT_REACHED) when PfR Manager tries to request ALL EXIT LINK REPORTS more than 2 times.

CSCsu84383 Router crashes with mlppp configs and on attaching/removing qos policy.

Symptom When policy from mlp vaccess is removed, router crashes in queuing enqueue.

Conditions Attach queuing policy to vaccess. Remove queuing policy from vaccess.

Workaround There is no workaround.

CSCsu95319 IGMP report was not sent to helper address.

Symptom Igmp-proxy reports for some of the groups are not forwarded to the helper. This causes members not to receive the multicast traffic for those groups.

Conditions The problem is seen when the igmp-proxy router is receiving UDP control traffic. That is, when the router is receiving any UDP control-plane traffic on any interface.

Workaround There is no workaround.

CSCsu98428 Crash with extraneous group-name configured on dial peer.

Symptom A router running Cisco IOS may reload unexpectedly.

Conditions This is seen on router with CME when a call is placed out of a dial-peer with a group-name configured when it is not defined globally. For example:

dial-peer voice 2 pots

group-name test

destination-pattern 9T

port 0/3/0:23

forward-digits all

Workaround Since the group-name has no functionality without anything defined globally, remove the config.

Further Problem Description: When configuring the group-name, a warning will appear if the config is incomplete:

Router(config-dial-peer)# group-name test

Warning: group test is not defined

but the configuration will still be accepted.

CSCsv00168 strange chars on CLIs.

Symptom Junk values are being displayed on the router when characters/commands are inputted. For example, enter "enable", it shows "na^@^@"; enter "show version", it shows "h ^v^@e^@^r^@^@^@^@^@".

Conditions The symptoms are observed with Cisco IOS Release 12.4(23.2)T.

Workaround There is no workaround.

Further Problem Description: The CLI function is not affected by the junk values.

CSCsv17687 Repeater client is not associated to root AP.

Conditions Configure a root ap, repeater AP and a client associated to repeater AP with leap/wep.The repeater client is not associated to root AP.

Workaround There is no workaround.

CSCsv20058 CUBE - duplicate H245-alphanumeric at digit_end on rfc2833 to h245-alpha.

Symptom Upon digit_end on the RFC 2833 side, the IPIP GW detects misinterprets this and sends out h245-alphanumeric which is duplicate. Typically, IPIPGW should ignore all the tone packets after the digit_begin is detected till the digit_end.

Conditions RTP-NTE to H245-Alphanumeric conversion is triggering this event.

Workaround There is no workaround.

CSCsv22171 wrong callerID on CME phone after put into conf by CM phone.

Symptom A CME phone may display it's own directory number after being put into a conference by a Communications Manager phone.

Conditions The topology is as follows:

ph1---CME----sip.Trunk-----CM-----ph2,ph3

ph2 puts ph1 into conference with ph2, and ph3.

Workaround There is no workaround.

CSCsv24862 GPickUp soft-key not working on xfer from CUE to parallel hunt group.

Symptom In CME 7.0 (12.4(20)T, transferring out of CUE Auto Attendant to a parallel hunt group on CME, and trying to pick up that call using the GPickUp soft-key doesn't work.

Workaround Use longest idle or sequential hunt group.

CSCsv35663 TrnsfVM using speed-dial, watched or monitored lines doesn't work.

Symptom Unable to transfer calls directly to voice-mail using the "TrnsfVM" soft-key followed by a speed dial, "watch" or "monitor" button on CCME running 12.4(20)T IOS.

Conditions Transferring calls directly to voice-mail using "TrnsfVM" soft-key followed by a speed dial, "watch" or "monitor" button.

Workaround Use:
http://www.cisco.com/en/US/customer/products/sw/voicesw/ps5520/products_tech_note09186a00802ab979.shtml

CSCsv42721 Association failure between client and UUT configured for EAP-TLS.

Symptom UUT configured as AP with EAP-FAST configurations fails to associate with the PC client (with appropriate profiles in place). The 'sh dot11 assoc' output shows that STateis struck at "AAA_Auth".

Symptom Association fails between with UUT/AP and PC clietn with EAP-TLS configurations.

Workaround There is no workaround.

CSCsv43444 Memory leak in ccsip_new_scb.

Symptom A router will run out of memory when SIP phones register.

Conditions Cisco 3911 phones are installed.

Workaround Disable MWI.

CSCsv49500 INVITE with + is converted to type international and + is stripped.

Symptom SIP INVITE messages sent to a router where the SIP URI and To header contain a number that begins with the plus sign (+) (e.g. +19195551234), do not match valid dial peers that have a + (e.g. destination-pattern +1919.....).

Conditions Occurs for any SIP call where the URI begins with a + and the dial peer to be matched begins with +.

Workaround If possible, remove the + from the dial peer to be matched.

An alternative is to create an inbound dial peer with a voice translation rule that matches on the international number and adds the + back on.

CSCsv51150 Stalled phone sockets are not cleaned up, SCCP process memory increase.

Symptom Skinny Msg Server process increases its memory usage eventually crashing the router.

Conditions SCCP devices trying to register while not in SRST mode

CSCsv53235 3911 type missing in voice register global load types.

Symptom 3911 is not a valid phone type under voice register global load commands.

Conditions A voice register pool is configured with a 3911 type.

Workaround Have both the pool and the load command use the 3951 type.

CSCsv58300 qos pre-classify not working in a DMVPN with tunnel protected with IPSEC.

Symptom Classification is not done correctly, it is matching the IPSEC header instead of matching parameters in the original header despite qos pre-classify configuration.

Conditions It has been observed in a DMVPN spoke, GRE tunnel with ipsec protection configured with qos-preclassify and applying service policy to the physical interface.

Workaround Classify traffic in ingress service-policy marking the traffic. Classify traffic in the egress with the mark inserted in ingress policy.

CSCsv60866 ringing pickup failing from dn's with "A." secondary numbers.

Symptom Picking up a ringing call fails and the original caller gets stuck afterwards.

Conditions The picking up phone has a dn configured with a secondary of the form "A."

Workaround Remove the secondary.

CSCsv75948 NTP crashes after fix of CSCsu24505.

Symptom Sending control packets to read the associations and peer, system variable from the router would crash the router.

Conditions The crash occurs only on generation of control packets to the router.

Workaround Don’t generate control packets to router.

CSCsv90212 SNR: Disable SCCP auto hold while SNR feature is not active.

Symptom After X + Y timer expires, the phone will stay in hold state.

Conditions SCCP phone is voice hunt group member and SNR enabled.

Both SNR and mobile phones are SNR enabled.

Workaround Disable the SNR feature under ephone-dn.

CSCsv95576 CME should translate #DEVICENAME# in XML URL reply for phones.

Symptom Phones on older firmware versions and non third-generation phones may not properly send their devicename if #DEVICENAME# is in the **CME <cmdBold>services url</cmdBold>** command.

Conditions The CME is version 4.2 or later, and in the phone's downloaded .cnf.xml file, the services url is similar to:

<servicesURL>http://<IP>:80/CMEserverForPhone/serviceurl</servicesURL>

This indicates that the phones will rely on CME to properly parse the #DEVICENAME# field for them, which it does not do in 12.4(20)T.

Workaround Downgrade CME to 4.1 or earlier, or manually edit the .cnf.xml files <servicesURL> field to the desired URL. Manually changing the field requires for the TFTP files to be statically maintained off of the CME as CME will rewrite the files and delete the non-default servicesURL field. This functionality is correctly working in CUCM deployments.

CSCsv99411 create-cnf file with 250 phones freezes console for 2 minutes.

Symptom Router appears to be hung when creating cnf-file for 250 phones with perphone configuration.

Conditions cnf-file location is set to flash and cnf-file is set to perphone.

Workaround There is no workaround, the system in fact is not hung, it is just busy waiting for io access to the flash. Will output progress indicator to the console screen to alert user to that.

CSCsw20408 SNR: hw conf did not work properly when mobile first answer the call.

Symptom After resuming the call from SNR phone, no voice path between conference parties.

Conditions Phone A calls SNR phone.

- SNR's mobile phone M answers the call, SNR phone is in auto-hold state.
- Phone A hw conference phone C.
- Press resume on SNR phone results in connection between SNR phone and mobile phone (M).

Workaround There is no workaround.

CSCsw25514 7914 fails to re-register after 'reset' is issued on CME 4.3.

Symptom On CME 4.3/7.0, when issuing a 'reset' for a 7960 with a 7914 sidecar, the 7914 will fail to re-register to CME and will stay with all buttons red.

Conditions This is observed on CME 4.3 and 7.0 for the 7960 with the 7914.

Workaround Downgrade to 12.4(15)T7 (CME 4.1) where the issue is not seen. Another workaround is to rebuild the CNF files with the below commands. This will allow for the device to be reset a single time and register properly. Successive resets will fail until the CNF files are rebuilt again.

CME#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

CME(config)#telephony-service

CME(config-telephony)#no create cnf-files

CNF files deleted

CME(config-telephony)#create cnf-files

Creating CNF files

CSCsw26371 park-system application * pickup conflicting with night-service codes.

Symptom **pickup + '*'** to retrieve the last parked call needs to be followed by **#** to work.

Conditions Set **night-service code** under **telephony-services**. This is applicable only to sccp phones.

Workaround Do not use **night-service code** or do **pickup + '*' + '#'**.

CSCsw28593 Intermittent Memory Block overrun and core after Hold and Resume.

CSCsw29421 cme crashed after cbarge/park the call.

Symptom image crash.

Conditions cbarge park the call.

Workaround There is no workaround, except to not do cbarge park.

CSCsw38175 Can't both calling/called sides cbarge into the call for SIP sharedline.

Symptom Unable to cbarge into sip shared line call that is already part of another cbarge conference created on another shared line.

Workaround There is no workaround.

CSCsw98091 Incoming SIP call with prefix dialing, always busy.

Symptom Call to SIP phone may return SIP 404 message.

Conditions When **dialplan-pattern** is configured under "voice register global", and someone from same or another CME dials the "expanded" number.

Workaround Do not configure **dialplan-pattern**.

Additional References

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

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.4(22)YB.

- *Cross-Platform Release Notes for Cisco IOS Release 12.4)T*
- *Cisco IOS Software Releases 12.4 Special and Early Deployments*
- *Caveats for Cisco IOS Release 12.4(22)T*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco IAD2801 series routers are at:

http://www.cisco.com/en/US/products/ps7214/tsd_products_support_series_home.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.

Notices

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

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