Release Notes for Cisco 800 Series Integrated Services Routers with Cisco IOS Release 12.4(11)XW

First Released: May 4, 2007
Last Revised: February 5, 2009
Cisco IOS Release 12.4(11)XW10
OL-13461-08 Eighth Release

These release notes describe new features and significant software components for the Cisco 800 series routers that support Cisco IOS Release 12.4(11)XW. These release notes are updated as needed. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* and *About Cisco IOS Release Notes*.

For a list of the software caveats that apply to Cisco IOS Release 12.4(11)XW**,** see the "Caveats" section on page 6, and the online *Caveats for Cisco IOS Release 12.4T*. The caveats document is updated for every 12.4T maintenance release.

Contents

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

System Requirements

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

Memory Requirements

Table 1 lists the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Cisco IOS Release 12.4(11)XW on the Cisco 800 series routers.

Table 1 Memory Requirements for the Cisco 870 Series Routers

Platform	Image Name	Image	Flash (MB) Recommended[1]	DRAM (MB) Recommended
Cisco 831	Cisco 831 Series IOS IP/FW 3DES	c831-k9o3y6-mz	16	64
	Cisco 831 Series IOS IP/FW 3DES		12	64
Cisco 836	Cisco 836 Series IOS IP/FW/Plus ISDN Dial BKUP 3DES VPN	c836-k9o3s8y6-mz	16	64
	Cisco 836 Series IOS IP/FW/PLUS 3DES	c836-k9o3sy6-mz	16	64
	Cisco 836 Series IOS IP/FW 3DES			
Cisco 837	Cisco 837 Series IOS IP/FW/PLUS 3DES	c837-k9o3sy6-mz	16	64
	Cisco 837 Series IOS IP/FW 3DES	c837-k9o3y6-mz	16	64
Cisco 851, Cisco 857	Cisco 850 Series IOS Advanced Security	c850-advsecurityk9-mz	20	64
Cisco 871, Cisco 871, Cisco 876, Cisco 877, Cisco 878	Cisco 870 Series IOS Advanced IP Services	c870-advipservicesk9-mz	24	128
	Cisco 870 Series IOS Advanced Security	c870-advsecurityk9-mz	24	128
Cisco 876	Cisco 870 Series IOS Advanced Enterprise Services	adventerprisek9-rnz	28	128

1. Recommended memory is the memory required considering future expansions.

Hardware Supported

Cisco IOS Release12.4(11)XW supports the following routers**:**

- Cisco 871
- Cisco 876
- Cisco 877
- Cisco 878

For detailed descriptions of new hardware features and which features are supported on each router, see the "New and Changed Information" section on page 4. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 800 series routers, which are available at

http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html

Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco 800 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

This section contains the following information:

New Hardware Features in Cisco IOS Release 12.4(11)XW10

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XW10

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XW9

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XW9

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XW8

There are no new hardware feature in this release.

New Software Features in Cisco IOS Release 12.4(11)XW8

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XW7

There are no new hardware feature in this release.

New Software Features in Cisco IOS Release 12.4(11)XW7

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XW5

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XW5

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XW3

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XW3

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XW2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XW2

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(11)XW1

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(11)XW1

There are no new software features in this release.

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

There are no new hardware features in this release.

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

There are no new software features in this release.

New Features in Release 12.4T

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

Limitations and Restrictions

There are no known limitations or restrictions in this release.

Caveats

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

This section contains the following caveat information:

Open Caveats - Release 12.4(11)XW10

There are no open caveats in this release.

Resolved Caveats - Release 12.4(11)XW10

- 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.

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsm97220

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCso05337

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsv38166

  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.

  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.

- CSCsk64158

  Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml.

- CSCsw24700

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

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

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

- CSCso04657

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

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

`CSCin76666 H.245 listener socket closed before H.245 connection is established.`

Symptom Intermittent outbound call failures using CallManager and Outbound Fast Start.

Conditions CallManager receives an inbound H.225 Facility message with startH245 at the same time as CCM transmits an H.225 Facility message with startH245. CCM closes the outbound H.245 TCP socket per H.323 Spec. Because the GW also closed the H.245 TCP socket it created, H.245 negotiation will halt and the call will fail.

Workaround Disable outbound fast start and this problem will not occur.

`CSCse59336 Three way call conferencing is not working properly.`

Symptom MGCP three-way call conferencing may fail because of an abrupt onhook event at the originating endpoint.

Conditions This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.13) and that is configured for voice calls over the Media Gateway Control Protocol (XGCP).

Workaround None.

`CSCsg35148 Interim record is sent with stop-only acct-list from RADIUS.`

Symptom Interim record is seen.

Conditions Conditions:stop-only ppp-acct-list is downloaded from merit RADIUS server.

Workaround None.

`CSCsj04758 Wrong codec bytes on the SIP leg of ipipgw for SIP--->H323 (g726).`

Symptom Wrong codec bytes are displayed on the SIP leg of ipipgw for SIP--->H323 interworking.

Conditions Work codec bytes of "0" is seen when SIP--->H323 interworking is done when codec g726 codec is configured. Call goes through fine but wrong bytes are displayed.

Workaround None.

`CSCsj75250 crafted SCTP packet reloads router.`

Symptom Crafted SCTP packet may reset router.

Conditions Affects Cisco IOS devices running 12.4(15)T and later based trains.

Workaround If not using SCTP on the device an infrastructure ACL, denying SCTP traffic to the device can be applied inbound to all interfaces.

`CSCsk40676 C1812 12.4.15.T / certain packet sizes block inside interface of ezvpn conn.`

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

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

Workaround Disable LZS compression.

CSCsm45113 RIB installs duplicate routes for the same prefix

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

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

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

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

CSCsm49826 c7206VXR/NPE400 reloaded due to bus error running 12.4(15)T2 and T3.

Symptom H323 gateways crash under load.

Conditions Multiple H323 calls were made simultaneously.

Workaround Configuring the following CLI should prevent the crash:

c2691-15(config)#voice service voip

c2691-15(conf-voi-serv)#h323

c2691-15(conf-serv-h323)#no h245 simultaneous-connection-handle

CSCso47738 No Voice Path For SIP to H323 calls.

Symptom Gateway sends 200 OK with media direction as SENDRECV for a reINVITE with offer having media direction INACTIVE.

Conditions This is seen for the supplementary services when the call is put on HOLD and then RESUMED.

Workaround None.

CSCso80830 W button should be lit on for undefined primary ephone.

Symptom The Watch button is not lit on if no watched phone for this watched DN. Ring back tone is heard when calling to this DN.

Conditions No phone, no matter registered or not, is configred with the watched DN.

Workaround None.

CSCsq04046 GUI: IOS SYSfeature undefined" error seen on help->about.

Symptom Error when accessing CME GUI Help->About page.

Conditions Using IOS image with feature variable more than 50 characters.

Workaround None.

CSCsr27960 Traceback observed after configuring credential under sip-ua.

Symptom Traceback observed when configuring credentials CLI under sip-ua.

Conditions This happens when user configures credentials CLI with username length more than 32 characters.

Workaround None.

CSCsr78883 Router console displays messages "Data corruption Data Inconsistency.

Symptom There will be traceback on configuring **mls qos cos pass-through dscp** in supporting interface mode.

Conditions Configuring "mls qos cos pass-through dscp" in the interface that supports the functionality.

Workaround Currently, the CLI is not supported in most network modules, and thus, is invisible to the users. If the CLI is supported, configure it as **mls qos cos override | cos-value** </B>

Further Problem Description: Due to the buffer overflow, there will be traceback when configuring the QoS in the supporting interface. Currently, the CLI is not supported in most network modules, and thus,is invisible to the users.

CSCsu36827 CUE clock does not sync up with the CME using NTP.

Symptom The CUE clock does not synch up with the 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.

CSCsu59847 The Content-Type used by T.37 should use a mutipart subtype of "mixed".

Symptom Certain mail clients may experience problems viewing the TIFF attachments sent by a Cisco T.37 OnRamp gateway because they do not support the Content-Type of multipart/fax-message that Cisco uses in it's T.37 Store-and_forward Fax implementation.

Conditions This problem should not affect most mail clients because Cisco is not in violation of any specifications. The MIME specification (RFC2046) clearly states that a mail client should treat an unrecognized subtype of multipart as being equivalent to the well known and widely used Content-Type of multipart/mixed.

Workaround None.

CSCsw50802 Smart Init Fails to recognize HWICs with smart cookie.

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

Conditions When HWIC is equipped with smart cookie.

Workaround Using static I/O mem configuration instead.

Open Caveats - Release 12.4(11)XW9

There are no open caveats in this release.

Resolved Caveats - Release 12.4(11)XW9

CSCsq13348

The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

NOTE: This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks. Cisco Systems has published a Cisco Security Advisory for that vulnerability, which can be found at http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml.

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

CSCek52673 Single crafted udp packet reloads router with dhcp server

Symptom A router that has DHCP server enabled could reload after receiving a malformed UDP packet.

Workaround There is no workaround.

CSCek71149 Error message when **dir** is issued

Symptom "Error getting file system status (Unknown error 0) or (Bad file number)" was observed when **dir <archive/system/tmpsys:>** was issued. The rest of the file systems have no problem (i.e. **dir nvram/flash/usbtoken0:**... etc)

Conditions Load routers with problem releases.

Workaround There is no workaround.

CSCsg42546 Reload when MGCP CRCX has sRTP and V150 params in LCO

Symptom An MGCP gateway reloads when receiving Secure Real-Time Transport Protocol (SRTP) and V.150 parameters in the local connection options of a Create Connection (CRCX) message.

Conditions This symptom has been observed when the gateway is configured to use SRTP and V.150 protocols.

Workaround Disable the use of either SRTP or V.150 protocol in the gateway.

CSCsj32422 CBWFQ:Unable to reconfigure the policy map after exceeding the bandwidth

Symptom Once policy map is configured and bandwidth is exceeded while dividing amongst the classes, re-configuration of the policy map is not possible.

Conditions Create a policy map, exceed the bandwidth amongst the classes (e.g. try to divide more than 75% in CBWFQ).

Workaround Don't exceed the bandwidth while configuring the policy map.

CSCsj50773 High cpu when querying ipRouteTable MIB

Symptom Performing the snmpwalk on the ipRouteTable MIB may cause high CPU and reloads.

Conditions This symptom is observed on a router that is running Cisco IOS Release 12.4(13b) or later releases.

Workaround Create a view that excludes the ipRouteTable:

snmp-server view cutdown 1.3.6.1.2.1.4.21 exclude

snmp-server view cutdown internet included

snmp-server community <comm> view cutdown RO

This view restricts the objects that the NMS can poll. It excludes access to the ipRouteTable, but allows access to the other MIBs.

CSCsj82622 Crash editing ACL cce_dp_named_db_ip_access_list_impure

Symptom A router may crash when you configure an access control list (ACL) that has at least 50-60 ACEs (about 100 nodes) that is used in policy maps that are already applied to an interface or when you boot the router after having made the configuration change. When the crash occurs, the following error message is generated: %ALIGN-1-FATAL: Corrupted program counter pc=0x0 , ra=0x0 , sp=0x66EFB8A0

Conditions This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(15)T or Release 12.4(15)T1.

Workaround There is no workaround.

CSCsk27147 SNMP stops responding while polling from CISCO-MEMORYPOOL-MIB

Symptom The following SNMP is incorrectly generated:"%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full". This issue is affecting the CISCO-MEMORYPOOL-MIB instead.

Conditions Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because of the input queue being full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the snmp process takes 5-20% of the CPU load.

Workaround Exclude ciscoMemoryPoolMIB from your query with the following commands:

snmp-server view public-view iso included

snmp-server view public-view ciscoMemoryPoolMIB excluded.

Apply this view to the RW community string. This view will exclude only ciscoMemoryPoolMib, all other MIBs will be available.

CSCsk39642 router crash when copying saved config to running config

Symptom A router crashes.

Conditions This symptom is observed when you are running Cisco IOS Release 12.4(17) or Release 12.4T and when you copy the saved configuration to the running configuration.

Workaround There is no workaround.

CSCsk94676 dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH

Symptom Transparent bridging into DLSw does not work.The following messages are displayed:

*Jan 29 19:00:50.727: %COMMON_FIB-4-FIBHWIDBMISMATCH: Mis-match between hwidb DLSw Port0 (ifindex 5) and fibhwidb GigabitEthernet2/3 (ifindex 5)-Traceback= 407C7004 407C8A38 407C7CEC 407C7EE4 413C9900 41BCE138 41BCCD54 41BCCFA8 41BCA330 413C0128 413C0114

*Jan 29 19:00:50.727: %COMMON_FIB-4-FIBMISSINGHWIDB: No fibhwidb while initializing fibidb for DLSw Port0 (if_number 5)

-Traceback= 407C83D4 407C8A9C 407C7CEC 407C7EE4 413C9900 41BCE138 41BCCD54 41BCCFA8 41BCA330 413C0128 413C0114

Conditions When using DLSw+ together with transparent bridging.

Workaround For a workaround, all transparent bridging commands related to **dlsw** can be replaced with DLSW Ethernet redundancy.

i.e.

As global command:

no dlsw bridge-group X

and on the interface:

no bridge-group X

on the interface replace it with:

dlsw transparent redundancy-enable 9999.9999.9999

CSCsl70722 Router crash polling rttmon mib with active IP SLA probes

Symptom A router running Cisco IOS may crash due to watchdog timeout.

Conditions Occurs when IP SLA probes are configured and active for a period of 72 weeks. After this much time has passed, polling the rttmon mib for the probe statistics will cause the router to reload. Then the problem will not be seen again for another 72 weeks.

Workaround There is no workaround.

CSCsm17281 Router crashes when adding ACL line to Service Policy

Symptom Device running 12.4(17.6)T will crash after adding line to an access-list attached to a service policy

Workaround There is none.

CSCsm77199 DATACORRUPTION-1-DATAINCONSISTENCY HTTP_FIND_FLASH_FILE

Symptom If the HTTP secure server capability is present, Switch shows the error message "%DATACORRUPTION-1-DATAINCONSISTENCY: copy error" with tracebacks after initializing the supervisor. This error message can be verified in **show logging** output.

Conditions **ip http server** is configured.

Workaround Configure **no ip http server.** The switch functionality is not affected by this error message.The problem is cosmetic.

CSCso09539 ACK not sent to 200 OK from CUE during h323 slowstart -- sip delayed med

Symptom Incoming H323 slow start call to CME when forwarded to voicemail in CUE may result in no audio.

Conditions This problem was observed when CME did not send ACK to 200 OK response from CUE.

Workaround Use H323 Faststart.If incoming H323 calls need to be slow-start for video calls and calls to voicemail need to be faststart, enable H.450 call transfer feature and use two incoming dial-peers:

- One H323 dial-peer configured with "**incoming called-number <ephone-dn extension range>**" and H323 slowstart using voice-class h323.
- Another H323 dial-peer configured with "**incoming called-number <voicemail dn>**" and H323 faststart using voice-class h323.

CSCsq42134 JPN: 7921 XML Services are displayed as squares

Symptom 7921 directories are displayed as squires in CME Userlocale: JP environment.

Conditions 7921: 1.1.1

CME: 4.2 (IOS 12.4(11)XW7)

Locale File : CME-locale-jp_JP-4.1.0.1.tar

Workaround There is no workaround.

CSCsq44013 View used twice with logging enabled

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

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

The view is used twice rather than once.

Workaround There is no workaround.

CSCsq64715 EM login credential could be set to stack junk in error condition

Symptom EM login username and password may be set to random values in process stack in case the actual input from the phone is in an invalid format. And if both string picked up from the stack happen to match a username/password pair in a configured user profile, EM will login the user accidentally.

Workaround There is no workaround.

CSCsq67163 IPSLA RTP operation crashes the router

Symptom Scheduling of IP SLA RTP operation crashes the router.

Conditions This problem occurs only when IPSLA RTP operation is configured and is scheduled to run.

Workaround There is no workaround.

CSCsq74999 SCCP FXS ports connected to FAX machines lock up

Symptom FXS that have fax/modems connected intermittently fail. Once they are in this stuck state, an incoming call to them will not ring the line, there will be no output in **debug vpm sig**. Outbound calls/faxes typically still work.

FXS port must be SCCP controlled. The problem is likely to occur when the pots leg is disconnected before the voip leg. If this occurs the port can go into this "stuck" state. Any subsequent calls will not ring the fax machine on this port.

Workaround Temporary workaround is to "shut/no shut" the voice-port. This problem seems to be related to cisco fax-relay being invoked and it's interoperability with SCCP in this IOS version. Configuring:

voice service voip

fax protocol none

will prevent the problem from happening. Removing the SCCP config from the ports will prevent it from happening too.

CSCsr01058 SPLIT_DNS: Debug msg Forwarding back reply is missing

Symptom An IOS device configured as a DNS server is vulnerable to forged answer attacks. In this type of attack, a malicious user can cause the IOS DNS server to accept a forged answer that associates a name with an IP address chosen by the malicious user. This answer ends up in the cache of the DNS server.

This attack can be made more difficult by randomizing both the DNS transaction ID and the UDP source port number that the DNS server (the IOS device) uses to relay DNS queries for domain it is not authorized for.

Conditions The above symptom is seen on a router loaded with 12.4(19.18)T image and above.

Workaround In the case of IOS, when the IOS name server relays a query, the DNS transaction ID that is used is the original ID received from the client, and the source UDP port is always 53. To make the IOS DNS server more resilient and less vulnerable to DNS cache poisoning attacks, at the very minimum both the DNS transaction ID and the UDP source port number must be randomized. The use of bit 0x20 in DNS labels to improve transaction identity is also recommended.

This is a security issue. The problem, however, only exists for customers who are running the IOS DNS Server/Forwarder and this is presumed to not be the usual case.

`CSCsr18200 busy tone issue when receiving a 183 Message`

Symptom A busy tone is not heard when a 183 message is received before a 4xx busy message.

Conditions SIP Trunk architecture with Italtel SSW. The bug affects both 12.4(15)T and 12.4(11)XW software releases.

Workaround A patch is required, forcing the media off when a busy message is received.

`CSCsr71715 Call display missing when park or xfer HW conference call`

Symptom Caller ID and Call bubble missing when a HW conference call is parked or Xfere

Open Caveats - Release 12.4(11)XW8

There are no open caveats in this release.

Resolved Caveats - Release 12.4(11)XW8

- CSCsq58779

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

  Cisco has released free software updates that address this vulnerability.

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

`CSCse70333 CFwdAll erroneously reconfigured after disabling night service`

Symptom CFwdAll incorrectly appears after night service is disabled.

Conditions CFwdAll was initially configured via softkey and un-configured via CLI. On the same dn as CFwdAll was on, night service is enabled and disabled.

Workaround Remove CFwdAll via softkey or reload the router.

`CSCsj38755 Ping Fails over ATM interface.`

Symptom Ping fails over the atm interface while applying Quality of Service.

Conditions When we configure the qos on ATM interfaces on the back to back connected routers the ping fails.

Workaround There is no workaround.

`CSCsl26765 DTMF not detected by CUE if I/C call is txfer to ph with CFDWALL to VM`

Symptom On CUBE DTMF is not detected to stop prompt playback or record message.

Conditions When the REMOTE incoming call is transferred to SCCP phone with CFWDALL to CUE-VM, DTMF is not detected to stop prompt playback or message recording. If original caller was LOCAL and followed the same call sequence, then there was no issue

Workaround There is no workaround.

CSCsm23378 DTMF transcoding from rtp-nte to in-band fails for same codec

Symptom DTMF transcoding should be done between call legs if DTMF relay is different, even if voice codecs are the same.

Conditions If voice codecs are the same, but DTMF relay settings are different then no transcoding is done. But when voice codecs are different then transcoding is invoked, and DTMF is transcoded from rtp-nte to in-band.

Workaround There is no workaround.

CSCsm34706 CUBE sends fixed DTMF duration and ignores received H.245 User Input

Symptom CUBE sends a fixed 800 time units for every digit pressed (sent via RFC 2833) regardless of what it receives in the duration of a H.245 User Input field.

Conditions In H323-SIP interworking scenario on CUBE, for DTMF conversion from 245-alphanumeric to RFC2833, regardless of the duration received in H.245 User Input field, CUBE always sends a fixed 800 ms for every digit pressed (sent via RFC 2833).

Workaround There is no workaround.

CSCsm37093 CME 4.1after security is enabled 7970 will register with US locale.

Symptom After security is enabled locale in the phone 7970 cannot be changed.

Conditions Customer cannot leave security enabled and configure their locale on Cisco 7960 and Cisco 7940 do not present the issue as they have the firmware locally stored (flash)

CSCsm64258 ephone-hunt group does NOT present calls to overlaid DNs

Symptom When an ephone hunt-group is configured with 'present-call idle-phon', the ephone hunt-group skips the DNs which are configured as overlay.

Conditions The problem is observed under the following conditions:

- ephone hunt-group is configured with 'present-call idle-phone'
- DN is configured as overlay

Workaround Remove the 'present-call idle-phone' configuration from the ephone-hunt configuration and do not use overlaying.

CSCsm74560 phone does not look for network locale file for user defined languages

Symptom Wireless IP phone 7920 does not download the 7960-tones.xml files when user defined network locale is configure.

Conditions CME writes incomplete XML tags in the phone config file, for user defined language network locale. So phone cannot generate the query for the relevant network locale file.

Workaround Complete the following steps to resolve the problem:

a. Along with User defined, we also need to define inbuilt network locale. For example:
   - DE - Germany
   - telephony- service
   - network- locale DE
   - create cnf- files
b. Rename the user defined file to 'germany_7960-tones.xml'.
c. Replace the file under ITS directory with the new 'germany_7960-tones.xml' (Make sure the name is the system defined name).
d. Do not run 'create cnf-file' as it will again override with the system defined parameters.
e. Reboot the 7921 wireless phone.

In case if you have issue in 'create cnf-file', then ensure to repeat all the steps mentioned above again.

CSCsm88771 CME trunk optimized calls being put on hold automatically

Symptom Answering a trunk call transferred from another phone is automatically put on hold and cannot be resumed.

Conditions The call originally came in on a trunk dn and is transferred to another extension on a phone sharing that trunk. Trunk optimization takes place.

Workaround There is no workaround.

CSCsm89158 7921 does not display call park number while the call is parked

Symptom 7921 does not show the parked number when the call is parked.

Conditions UC520W-16U-4FXO-K9 and 7921(CP7921G-1.0.3.LOADS)

Workaround There is no workaround.

CSCso25982 SIP transfer at connect with No Audio

Symptom No audio when one SIP extension transfers a call from PSTN side to second SIP extension.

Conditions The call flows from PSTN to SIP Extension-A, transfer at connect to SIP Extension-B.Make a call from PSTN to DID number of SIP extension-A, extension-A answers. SIP extension-A transfer-at-connect to SIP extension-B, Extension-B answers. Extension-A completes the transfer by pressing transfer button. PSTN and Extension-B gets connected but NO AUDIO.

Workaround There is no workaround.

CSCso26056 SIP Extension unable to transfer at alert to a PSTN number

Symptom SIP(XOR) extension is also UNABLE to retrieve the call to PSTN-A(XEE) (hold state).

PSTN-A(XEE) remains in hold state.

Conditions "No supplementary-service sip refer" XEE coming to CME through SIP trunk, to SIP phone XOR, consultation transfer to XTO going out through SIP trunk. The SIP trunk dial-peer has same destination pattern as pots dial-peer, and pots dial-peer needs to have preference lower than SIP trunk dial-peer.

Workaround Use "supplementary-service sip refer" or remove pots dial-peer with same destination pattern or make SIP trunk dial-peer preference lower than pots dial-peer.

CSCso27097 One way audio after xferring incoming SIP trunk call with transcoder

Symptom One way audio after transfer.

Conditions XEE SIP trunk or phone, XOR SIP Phone, XTO sccp. XEE codec is different from XOR codec, using transcoder.

Workaround Try to use same codec.

CSCso36239 wrong primary-phone observed after re-configure primary-dn of the ephone

Symptom Wrong primary-phone observed after re-configure primary-dn of the ephone

Conditions Wrong primary-phone observed after re-configure primary-dn of the ephone

Workaround There is no workaround.

CSCso39201 ephone gets into DND mode while in Connected state

Symptom 7961 and 7941 phones going into DND mode in Connected state.

Conditions User getting incoming call on 7941 and 7961 phones. Since the softkeys do not update fast, if the user presses DND immediately after going into connected state then after going onhook the user phone would stuck in DnD mode.

Workaround There is no workaround.

CSCso42145 CCME ephone name config result in called number display issue

Symptom IP phone is displaying the calling name in placed of called name for an incoming call from PSTN.

Conditions The problem exists in 12.4(15)XW code.

Workaround There is no workaround.

CSCso45361 High jitter in ringback from CUE

Symptom External caller gets transferred from CUE to an internal DN number, and the ringback sent to the caller is distorted because of jitter.

Conditions Internal DN to Internal DN ringbacks on CUE are fine, only external calls.

Workaround There is no workaround.

CSCso56824 SCCP OOB-RFC2833 DTMF interworking issue for CME customer

Symptom RFC2833 DTMF packets are sent too fast to be processed by IVR systems.

Conditions Send DTMF tone via RTP-NTE.

Workaround There is no workaround.

CSCso64585 redundant CallRemoteMultiLine sccp msg to monitor park DN

Symptom Jitter or voice quality issue may occur.

Conditions If there are a lot of ephones, say there are 50, monitoring same park DN, there will be 2500 same sccp messages sent to these 50 phones respectively in few mili seconds.

Workaround There is no workaround.

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

Symptom After Reload, Secure Conference profile does not register with Cisco Call Manager.

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

Workaround Do not specify the truspoint when configuring Call Manger CCM using CLI "sccp ccm <ip address> tag version <x>.

CSCso74656 MG2:device-based BLF shown incorrect status for EM

CSCso78702 7961 IP Phone acct softkey get "no park number available"

Symptom 2851 Version 12.4(15)T4 press the ACCT SoftKey and get "NO PARK NUMBER AVAILABLE".

CSCso95643 sRTP Package missing in c1861

Symptom MGCP srtp-package option is not available in c1861 platform.

Conditions This occurs on Cisco 1861 only.

Workaround There is no workaround.

Open Caveats - Release 12.4(11)XW7

There are no open caveats in this release.

Resolved Caveats - Release 12.4(11)XW7

- CSCsk62253

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

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

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

- CSCsl62609

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

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

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

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

- CSCsk60020

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

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

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

  The Security Advisory for this issue is posted at

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

CSCsi55685- kron removes recurring tclsh cli after first run

Symptom The following recurring kron schedule fails and gets removed after the first run. kron occurrence tcl in 1 recurring policy-list tcl ! kron policy-list tcl cli tclsh disk0:hello.tcl!

Conditions enter the following configuration commands: kron occurrence tcl in 1 recurring policy-list tcl ! kron policy-list tcl cli tclsh unix:hello.tcl ! create a file on disk0: called hello.tcl with the following contents: puts "hello"

Workaround None

CSCsk25697- unprotected buginf may cause cpuhog under repeated udp traffic to 53

Symptom A router with DNS server configured may show CPUHOG tracebacks when it receives repeated crafted udp packets to its port 53. Sample for 3800 router: %SYS-3-CPUHOG: Task is running for (40004)msecs, more than (2000)msecs (5/0),process = DNS Server Input. -Traceback=0x60D68CDC 0x6033D984 0x6180E58C FFFFFFA0 3F 4E 60 0x708DFD18 06 FFFFFFFE FFFFFF88 FFFFFFA5 FFFFFFA3 FFFFFF92 FFFFFFA7 FFFFFF8B 7A 3A FFFFFFF5 17 FFFFFF9B FFFFFFC9 FFFFFF9B FFFFFFA2

Conditions Router needs to have dns server configured and listen to udp port 53 conf t ip dns server end

Workaround Apply rate limit to port 53 to interfaces facing untrusted networks: access-list 100 permit udp any any eq domain access-list 100 deny ip any any interface GigabitEthernet0/0 ip address 10.2.2.2 255.255.255.0 rate-limit input access-group 100 8000 1500 2000 conform-action transmit exceed-action drop.

CSCsl48237- incorrect bounding length in sstrncpy() calls in l2tp files

Symptom If a large name string is used when configuring the command "security crypto-profile" under the l2tp-class submode, we could have a buffer overflow which may crash the router.

Conditions This problem only occurs if a large name string is used in the "security crypto-profile" command.

Workaround There is no workaround.

CSCsl59294- %DATACORRUPTION-1-DATAINCONSISTENCY at caplog_logger_proc

Symptom A Cisco router may see the following error once shortly after bootup: *Nov 21 15:16:28 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x416DE178 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE178 0x416DE650 0x423E303C 0x423E3020 *Nov 21

15:16:28 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x416DE188 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE188 0x416DE650 0x423E303C 0x423E3020 No functional impact is seen.

Conditions Occurs on a Cisco 2811 router running Cisco IOS Release 12.4(13d).

Workaround Disable the following configuration on the router: **voice hpi capture buffer***size* **voice hpi capture destination** *filename*

CSCek41543- Cisco2811 Processor Pool Memory Leak in ISDN and Crash

Symptom A Cisco 2811 router running Cisco IOS Release 12.4(7a) may have a memory leak in the ISDN process as has been seen in the **show process memory**. The leak rate appears to be about 1.20MB/Hour.

Conditions This symptom has been observed with BRI-U interface that is UP/UP (spoofing).

Workaround Administratively shut down the BRI interface.

CSCsi21389- One-way multicast traffic over wireless.

Symptom Routers that have the ability to use the optional 802.11b/g card, such as the Cisco ISR series do not pass multicast traffic across the wireless interface.

Conditions Cisco routers that have the 802.11 b/g HWIC card do not pass multicast traffic across the wireless interface, though multicast routing is enabled and otherwise is configured normally. Wireless hosts cannot pass multicast traffic between each other, and multicast traffic from the wired network will not be transmitted out the wireless interface.

Workaround None

CSCsi44510- CME multicast audio to the 7921 cuts out on HWIC-AP

Symptom Multicast audio to the 7921 cuts out after a few seconds and will not resume.

Conditions A 7921 registered to CME doing multicast paging or multicast MOH

Workaround none

CSCsj14277- Wrong Calling ID by transfer, only with 7931 - 12.4(4)XC6

Symptom The caller id on the transfer-to is not updated with the transferee after the transferrer commits the transfer.

Conditions When the transfer-to answers the call from the transferrer, the caller id on the transfer-to shows that the call is from transferrer. After the transferrer commits the transfer, the caller id should be updated with the transferee. This caller id display issue can be observed if the transferrer DN is shared by the transfer-to.

Workaround There is no workaround without removing the XOR DN from the XTO.

CSCsj34770- Having problem in establishing QSIG Prime call

Symptom QSIG PRIME call is not going between slave and master routers

Conditions This issue is seen in 12.4(16.5)T

Workaround No workaround

CSCsj50982- Wrong isdn cause code while making call to wrong destination

Symptom Wrong isdn cause code coming while making call to wrong destination

Conditions While call made to wrong destination number

Workaround none

CSCsk25697- unprotected buginf may cause cpuhog under repeated udp traffic to 53

Symptom A router with DNS server configured may show CPUHOG tracebacks when it receives repeated crafted udp packets to its port 53. Sample for 3800 router: %SYS-3-CPUHOG: Task is running for (40004)msecs, more than (2000)msecs (5/0),process = DNS Server Input. -Traceback= 0x60D68CDC 0x6033D984 0x6180E58C FFFFFFA0 3F 4E 60 0x708DFD18 06 FFFFFFFE FFFFFF88 FFFFFFA5 FFFFFFA3 FFFFFF92 FFFFFFA7 FFFFFF8B 7A 3A FFFFFFF5 17 FFFFFF9B FFFFFFC9 FFFFFF9B FFFFFFA2.

Conditions Router needs to have dns server configured and listen to udp port 53 conf t ip dns server end.

Workaround Apply rate limit to port 53 to interfaces facing untrusted networks: access-list 100 permit udp any any eq domain access-list 100 deny ip any any interface GigabitEthernet0/0 ip address 10.2.2.2 255.255.255.0 rate-limit input access-group 100 8000 1500 2000 conform-action transmit exceed-action drop.

CSCsk71610- CCSIP_UDP_SOCKET causes high CPU Usage

Symptom Incoming and outgoing calls fail due to high CPU Usage.

Conditions CPU Usage is at 99-100% and CCSIP_UDP_SOCKET is using 88+%.

Workaround There is no workaround.

CSCsl18024- HWIC Country Code Issue

Symptom Error message %DOT11-3-POWERS_INVALID: Interface Dot11Radio0/3/0, no valid power levels available is displayed during boot up.

Conditions Occurs for certain HWIC-AP cards with wrong country code values

Workaround Work around is to use HWIC AP cards of correct country code values.

CSCsl59294- %DATACORRUPTION-1-DATAINCONSISTENCY at caplog_logger_proc

Symptom A Cisco router may see the following error once shortly after bootup: *Nov 21 15:16:28 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x416DE178 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE178 0x416DE650 0x423E303C 0x423E3020 *Nov 21 15:16:28 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x416DE188 -Traceback= 0x412593C0 0x41276250 0x412947F4 0x416DE188 0x416DE650 0x423E303C 0x423E3020 No functional impact is seen.

Conditions Occurs on a Cisco 2811 router running Cisco IOS Release 12.4(13d).

Workaround Disable the following configuration on the router: voice hpi capture buffer*size* voice hpi capture destination *filename.*

CSCsm04209- PVDM2-DM fails to initiate calls over EuroISDN BRI while TEI is inactive.

Symptom Modem calls fail to establish when 'isdn tei-negotiation firstcall' configured on ISDN interfaces.

Conditions The ISDN BRI interfaces are added to CSM signaling interface queue only when they are active (layer 2, MULTI-FRAME-ESTABLISHED). Since, the ISDN L2 is not activated until the first call is initiated which in turn means there is no signaling interface available, which results in call failure.

Workaround Add the ISDN BRI interfaces to CSM signaling interface if they are not administratively down (shutdown).

CSCsm45689- UC520 crashed when system test was executed with debug logs enabled.

Symptom UC520 crashed when system test was executed with debug logs enabled.

Conditions UC520 crashed when system test was executed with the below debug logs enabled. debug callmon core debug callmon info debug callmon detail debug ccsip message.

Workaround None.

CSCsm46227- Router crash with CPUHOG for trunk port monitoring.

Symptom Cisco 3845 may crash when there is an incoming trunk call.

Conditions Occurs if the shared trunk DN is monitored by a FXO port and it is call-forwarded to another trunk DN with "call-forward all".

Workaround None.

CSCsm49011- VG224 SCCP port plays reorder before CM routes call-IOS interdigit timer.

Symptom On an FXS port configured for SCCP usage (such as on a VG224), reorder is heard 10 seconds after the last digit dialed when a number is dialed that requires waiting for interdigit timeout on CallManager.

Conditions Using SCCP controlled FXS port on an IOS box. Dialing a number which requires waiting for interdigit timeout to route (such as a variable length international number).

Workaround Increase the interdigit timeout setting on each SCCP FXS port to 16 secs (to be greater than CallManager's 15 secs). This is done by configuring "timeouts interdigit 16" under each voice port. OR decrease the CallManager interdigit timeout to 9 seconds (to be less than the VG224 port's 10 secs). This is done by changing the CallManager service parameter T302 Timer value to 9000 msec (9 seconds). If this workaround is chosen the new interdigit timeout setting will apply to all devices attached to the CallManager, not just the IOS SCCP FXS ports.

CSCsm55045- Crash illegal deallocation of unassigned/in-use memory.

Symptom A Cisco router configured with Call Manager Express (CME) may reload due to point to illegal deallocation of unassigned/in-use memory.

Conditions Occurs when CME is enabled.

Workaround There is no workaround.

CSCsm50874- CME: calling name in facility IE doesn't display on IP phone.

Symptom CME 4.2 does not display calling name when sent in an ISDN facility IE message. The facility is received and interpreted correctly however it doesn't show up on the IP phone display.

Workaround IOS 12.4(11)XW3 and 12.4(15)XY correct display the calling name.

CSCsm65685- Need to enable vendorConfig parameters on 7912.

Symptom After the configuration of telephony-service service phone settings Access 2 <settingsAccess>2</settingsAccess>" is missing in system:/its/XMLDefault7921.cnf.xml.

Workaround None.

CSCsm92260- CSKU wrong country code issue.

Symptom Error message Feb 28 08:50:28.459: %DOT11-3-POWERS_INVALID: Interface Dot11Radio0/0/0, no valid power levels available seen on router console during router boot up.

Conditions Occurs for certain CSKU cards with wrong country code values.

Workaround Work around is to use CSKU cards of correct country code values.

CSCso33776- spurious access error in AFW_M_Destination_Initiate.

Symptom Spurious memory access messages may be generated by a router. Mar 28 02:45:02.016: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x41DCE7E0 reading 0x60 Mar 28 02:45:02.016: %ALIGN-3-TRACE: -Traceback= 0x41DCE7E0 0x41DCF674 0x41DD351C 0x41DD6BBC 0x41DA96CC 0x41E0E428 0x41E0F2C4 0x41DF36D4. This issue may be cosmetic in nature.

Conditions These spurious memory accesses may be triggered by a T1/E1 PRI call or other event.

Workaround There is no known workaround. This issue may be cosmetic in nature.

Open Caveats - Release 12.4(11)XW6

There are no open caveats in this release.

Resolved Caveats - Release 12.4(11)XW6

CSCsg91306

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

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

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

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

CSCsi17020

A series of segmented Skinny Call Control Protocol (SCCP) 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 http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml.

CSCsj85065

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

Cisco has released free software updates that address this vulnerability.

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

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

CSCsk42759

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

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

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

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

CSCso81854

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

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

Cisco has released free software updates that address these vulnerabilities.

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

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

Open Caveats - Cisco IOS Release 12.4(11)XW5

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XW5

CSCsk45804 CME speeddials fails after attempting to invalid number

Symptom Pressing a speeddial button on CME does nothing.

Conditions Previously, a speeddial was used to target an unavailable/non-existent number.

Workaround Connect a normal call on the problematic phone.

CSCsk65748 If POE 48V fails to come up, we need to retry 3 times

CSCsk60054 Configuration buffer full. Cannot display show run

Symptom When certain configuration changes, the running configuration might not be able to be displayed and the following error message might appear:

```
% Configuration buffer full, can't add command: !
 %Aborting Save. Compress the config, Save it to flash or Free up space on device
```

Conditions The issue is seen either using or not using service compress-config on a Cisco IOS Router running CallManager Express (CME) when configuring more than 22 voice user-profiles.

Workaround There is no workaround.

CSCsk31644 Spurious Access at cmm_crs_proc_tr_call_consult_resp

Symptom Spurious memory access is seen while executing call forward scenarios.

Conditions This is seen on c3845 while executing CME and UCCX related test scenarios.

Workaround There is no workaround.

CSCsk55078 CME 4.2 Diversion Header issue in chained supplementary service

CSCsk22265 CME: 7935 and 7936 Corporate Directory Lookup fails in CME 4.1 and 4.2

Symptom When attempting to use the Corporate Directory Lookup feature on a Cisco 7935 or 7936 Conference IP Phone, an attempt to search for matching records using a First Name or Last Name query results in the message "Server not found" being returned.

Conditions This behavior is observed when the Cisco 7935 and 7936 Conference IP Phones are registered to a Cisco Unified Call Manager Express (CUCME) Voice Router installed with CUCME version 4.1 or newer (IOS 12.4(15)T train and newer, or 12.4(11)XJ and newer). The 7935 and 7936 IP Phones can be installed either with the approved SCCP Firmware Version 7.x or 8.x phone loads.

Workaround (1) This problem is not observed in CUCME 3.3 (IOS 12.4 mainline) up to 4.0(2) (IOS 12.4(11)T3). If CUCME 4.1 features are not required use these older versions of CUCME. (2) Use a non-79x5 IP Phone registered to the same CUCME Voice Router to perform the Local Directory Search.

CSCsk50911 Need to update the max-ephones range for various platforms

CSCsk25651 ephone-dn removal does not clean up mwi state

Symptom With Cisco Unity Express (CUE) integrated to Cisco Unified Communication Manager (CUCM) / CallManager utilizing SRST functionality, when the IP phones are registered to the SRST router, the MWI states may be incorrect.

Conditions When a phone registers to an SRST router, each directory number (DN) gets a particular ephone-dn number that will have a particular MWI state. If the phone unregisters from the SRST router and later re-registers to the router (possibly due to an intermittent connectivity to the CUCM), the ephone-dn number may be different since the ephone-dn numbers are assigned sequentially in a first-come-first-served fashion. The MWI state, however, is remembered from the previous registration that used the ephone-dn number so the MWI status could be incorrect.

Workaround There is no workaround.

CSCsj53899 Remove xlate profile from voice register dn removes from dial-peer

Symptom Removing voice xlate profile from a voice register dn results in the same xlate profile being removed from a dial-peer.

Conditions Have the same xlate profile name under a voice register dn and dial-peer and using IOS 12.4(11)XW - XW2.

Workaround There is no workaround.

CSCsj93762 Resume fails after HOLD for SIP phones regist with voice-class codec

CSCsj81363 FRU incorrect and Carrier Set empty on wireless B sku platforms

Symptom Under the show controller output for the Dot11 interface, the carrier set field is empty. This should say Americas. This does not affect functionality, all of the correct channels are present. Under the show diag output, the FRU says CISCO1811W-AG-A/K9 instead of CISCO1811W-AG-B/K9. This is just the labeling and does not affect functionality.

Conditions This is seen with the B models of the 1800 wireless routers running 12.4(11)XW1.

Workaround There is no workaround. This issue does not affect functionality.

CSCsk42889 SIP call xfer to voicemail fails with DNS Query failed error

Symptom SIP trunk----CME/CUE AA---xfer extension---CFNA---CUE voicemail. Call transfers from AA to extension, CFNA back to CUE voicemail drop.

Conditions CME running 12.4(11)XW3.

Workaround There is no workaround.

CSCsk58359 Update max sip phone range for various platform

CSCse14595 call may be connected while being cfna to an PSTN call

Symptom CME allows call connect after CFNA timer expire. On the 3745 with IOS 12.4(5)a customer can pick up the phone and get connected to the calling party after the CFNA timer expire.

Conditions When this problem is seen then there is a delay between Call-proc and Alerting messages from ISDN side.

Workaround Use the longer CFNA timer or use the "application default.c.old".

CSCsk35315 CME: calledName= displayed garbled characters

Symptom Display on Cisco IP Phone contains corrupted characters when placing outbound PSTN call on an ISDN circuit.

Conditions A Cisco IP Phone placing an outbound ISDN call through a Cisco IOS gateway configured for Cisco Unified Communication Manager Express may experience at times the name displayed on the screen with unrecognizable characters once the call connects.

This can occur if there is an ISDN Facility message received after the call connects that does not contain display name information; for example an inbound facility message for Advice of Charge (AOC) may trigger this problem.

These messages can be seen on the gateway through the use of debug isdn q931. Caution should be taken when enabling any debugs on a production router/gateway as it can impact performance. Make sure as a minimum to disable console logging on the IOS device before enabling any debug. This issue does not have an impact to the operation or performance of the gateway nor phone.

Workaround Contact the ISDN service provider to determine if the facility messages causing this problem can be disabled.

CSCsk16153 Modem won't be disconnected on exit

Symptom Modem connection is still active on exit.

Conditions After "exit" from modem session.

Workaround There is no workaround.

CSCsk73035 dtmf stop working if using connection plar opx immediate on fxo port

Symptom dtmf stop working if using connection plar opx immediate on fxo port.

Conditions Cu is running 124-11.XW on uc520. the dtmf does not work in the following call flow:

```
pstn--fxo---gw--sip--cue AA

If removing "immediate" from the following config,
the dtmf works.

voice-port 0/1/0
connection plar opx immediate 111
caller-id enable
```

Workaround Don't use "immediate" option for the "connection plar opx".

CSCsk46424 Authentication fails on main dot11 interface when xconnect configured

CSCsk52683 System crashed when wireless client is trying to associate with AP

Symptom System crashes when there are clients trying to associate with AP.

Conditions When AAA authentication fails with mis-configuration in the system or the wireless client's password is given wrong to try to associate.

Workaround Make sure the AAA configuration is setup correctly and the client password is configured correctly.

CSCsk17498 Per Port Storm-Control is broken

CSCsj88854 Router crashes when a call is made from Remote Phone registered to CUCME

Symptom A call made over a SIP trunk from a remote phone registered to Cisco Unified Call Manager Express 4.1 to a phone registered to a SIP proxy server results in router crash due to memory overrun.

Conditions Phone call has to be from remote phone. MLPPP should be configured as the WAN link. SIP trunk also traverses the same WAN link.

Workaround Remove the MLPPP.

CSCsj02456 HTTP PUT operation using copy command failed

Symptom HTTP PUT operation using copy command failed.

Conditions Failure is seen with HTTP PUT operation using copy command.

Workaround There is no workaround.

CSCsk83795 call may be disconnected when resetting other ephone

Symptom Call is disconnected when another ephone is reset or unregisters.

Conditions The call on the ephone-dn shared by other phone as non monitor button is disconnected if it is reset or unregisters from the CCME.

Workaround There is no workaround.

CSCsj14565 ACL = deny; sa request ignored when crypto local-address is dynamic

Symptom After a reboot of the router, or sometimes during normal operation, an IPsec tunnel fails to initiate. When debug crypto ipsec is enabled, the following error can be seen in the debug output: IPSEC(sa_initiate): ACL = deny; sa request ignored.

Conditions The router is running 12.4(12) or later, and a crypto map name local-address interface statement is present in the configuration, where interface is the name of an interface that has a dynamic IP address configured (e.g. ip address negotiated or ip address dhcp)

```
For example:
crypto map mycryptomap local-address Dialer0
interface Dialer0
 ip address negotiated
```

Workaround A short term workaround consists of removing the access-list used in the crypto map, and then adding it again. This will bring up the tunnel as soon as there is an interesting traffic, but the problem may occur again later. Remove the crypto map name local-address interface statement, if possible. Downgrade to a release earlier then 12.4(12).

CSCsk74181 SIP DO-DO - Basic Fax call fails

Symptom Fax call fails for a SIP DO-DO call.

Conditions When the CUBE receives a ReINVITE with fax params, it does not forward the same. Instead it sends a BYE and the call gets disconnected.

Workaround There is no workaround.

CSCsl04993 uc520 devices does not get reload via SNMP

Symptom Cisco Unified Communications Series Integrated Services routers are not reloaded through SNMP.

Conditions Cisco Unified Communications Series Integrated Services routers (ISRs) are not reloaded using SNMP when you restore the device configuration. Cisco Monitor Manager sends a device-reload request to the device after configuration file is restored; however, Cisco Unified Communications 500 Series ISRs do not accept this request through SNMP.

Workaround To work around this problem, reload the device manually after restoring the configuration file.

CSCsj56438 Crafted EAP Response Identity packet may cause device to reload

Symptom This Cisco Bug ID identifies vulnerability in Cisco's implementation of Extensible Authentication Protocol (EAP) that exists when processing a crafted EAP Response Identity packet. This vulnerability affects several Cisco products that have support for wired or wireless EAP implementations.

This vulnerability is documented in the following Cisco bug IDs:

```
* Wireless EAP - CSCsj56438
* Wired EAP    - CSCsb45696 and CSCsc55249
```

This Cisco Security Response is available at the following link: http://www.cisco.com/warp/public/707/cisco-sr-20071019-eap.shtml.

CSCsk66907 %SYS-3-CPUHOG: due to Skinny MOH Server process

Symptom PU Hog due to Skinny MOH Server causing phones to unregister:

```
%SYS-3-CPUHOG: Task is running for (xxx)msecs, more than (xxx)msecs
(xxxxxx),process = Skinny MOH Server.x
```

Conditions Occurs if Music on Hold (MOH) is being streamed from flash in IOS 12.4(11)XW3.

Workaround Use the live feed option by plugging in a CD player or iPOD or any such device to the MOH port on the UC500. Disable MOH from flash that implies tone on hold (or beep on hold).

CSCsi60392 CME does not send SIP NOTIFY DTMF to CUE-AA after txfer from CUE-VM

Symptom No response to DTMF inputs during Auto Attendant session.

Conditions Remote caller (across SIP Trunk) leaves voice message on local subscriber's CUE and then gets transferred to local AA. AA requests DTMF input for prompts played but this is not detected by CUE.

Workaround There is no workaround.

CSCsl12443 CME: TNP phones may experience one way audio

Symptom IP phone with FXO trunk config may experience intermittent one way audio. Debug ephone detail will show the following error:

```
OpenReceiveChannelAck status orcError on socket
```

Workaround Reboot the phone.

CSCsj38652 Freddo DTMF/cptone issues for Taiwan, Hong Kong, Singapore Compliance

Symptom DTMF levels are 0.3-0.5 dB below minimum limits for DTMF high/low tone signal power for Taiwan, Hong Kong and Singapore.

Conditions This causes under normal conditions.

Workaround Setting the cptone on the voice port to Singapore cures the problem.

CSCsk83813 sip call will pick up the wrong codec type from voice class codec

Symptom When a SIP call is established, the Cisco IOS correctly uses the "codec preference 2" setting (G.711ulaw) that is configured in the voice class codec configuration. When this problem occurs, the tone remote control functionality does not work and voice becomes distorted due to the codec mismatch.

Conditions A SIP call consistently uses the incorrect codec type from the "voice class codec" configuration. It should use the value that is configured for "codec preference 1," instead it uses the value that is configured for the "codec preference 2" setting. This issue occurs when the following configuration is used:

```
voice class codec 1
      codec preference 1 g729r8
      codec preference 2 g711ulaw

dial-peer voice 9191916 pots
 description #1/1:16#0# INUSE 163
 destination-pattern 19900001429191916
 port 1/1:16

dial-peer voice 555 voip
 rtp payload-type lmr-tone 107
 rtp payload-type nte-tone 108
 voice-class codec 1
 session protocol sipv2
 incoming called-number.
 dtmf-relay rtp-nte
 no vad

Using 2811
Cisco IOS versions: 12.4(17.4)PI1b and 12.4(17.4)PI1a
```

Workaround There is no workaround.

CSCsk63037 CME 4.2 has broken caller ID feature

Symptom Calling name is corrupted for ISDN calls on CME.

Conditions The problem can be seen for every call.

Workaround There is no workaround.

CSCsk95708 10 to 30 sec delay in starting media in secure meet-me conference

Symptom SCCP messages are delayed by a few seconds for secure calls, this could effect secure dspfarm secure analog endpoints.

Conditions Using secure dspfarm or analog endpoints.

Workaround There is no workaround.

CSCsk42180 Few Objects of CISCO-LICENSE-MGMT-MIB giving wrong values during SNMP wa

CSCsj94818 C877: ADSL2+ AnnexM: PVC goes to INAC after QoS is applied

Symptom On C877 device for VC which is configured with vbr-nrt and PCR rate higher that VC bandwidth, when changes are introduced (e.g. QoS applied), VC goes in INAC status due to the fact that PCR is higher than physical bandwidth.

Conditions Problem is seen on C877 device with ADSL2+ and with SW releases 12.4(11)XJ3 and 12.4(15)T1.

Workaround Resetting VC resolve issue.

CSCsk06443 SIP TGW sends 183 response even though no response from ISDN

Symptom IOS Gateway is sending 183 Response upon receiving retransmission of Invite Request.

Conditions IOS GW has sent 100 trying response to original Invite Request and the call is in progress on other leg. Other leg could be either PSTN OR IP.

Workaround There is no workaround.

CSCsk36600 Router crashes when ExtACL has mixed of tcp host and tcp net with QoS

Symptom Router might crash when Extended ACL is applied with mixed of tcp permit statements with host and networks and this acl is applied in the class-map.

Conditions The crash is seen when QOS with this Extended ACL is configured first and ACL statements are defined later.

Workaround Configure permitted host statements successively and do the same for permitted networks. Configure ACL statements first and attach this ACL to class-map later.

CSCsj80906 Router crashes on changing ACL linked to service policy

Symptom A Cisco router may crash due to a bus error.

Conditions This has been experienced on multiple Cisco router platforms running IOS release 12.4(15)T1. The crash can occur if an access-list linked to a service-policy is removed, or if a service-policy is removed on an interface.

Workaround There is no workaround.

CSCsl17037 CME: Local Directory Issue

Symptom Directory numbers that are configured in local directory of CME are not being shown in received calls directory. The number and name shows while call in ringing state but is not showing during connected state.

Conditions This is seen in Inbound call.

Workaround There is no workaround.

CSCsl04115 CM call to CME when Put on Hold, CME Hears FastBusy instead of TOH

Symptom Cisco IP Phone placed on hold hears fast busy instead of tone-on-hold.

Conditions A Cisco IP Phone registered with a Cisco Unified CallManager Express (CME) may hear a fast busy tone when placed on hold. This can occur when interworking with Cisco Unified CallManager (CCM) as shown here:

```
IPPhoneA---CM---H323---CME---IpPhoneB

-  Phone A calls Phone B
-  Phone A puts Phone B on Hold.
-  Instead of playing Tone On Hold, Phone B user hears a fast busy tone.
```

Workaround This behavior was introduced in 12.4(15)T. Either downgrade the IOS version on the CUCME or configure music-on-hold (MOH) to be played from CUCM, instead of TOH.

CSCsk72582 Call in B-ACD drops if answered after hunting second time round

Symptom Calls in B-ACD on CME router drops if the first round hunting is done through the hunt group lines. If the call is not answered, the caller is placed in the queue and hears an announcement with "all agents busy please hold " and so on. When the script hunts again after a timeout and this time, the call is answered, it drops the call completely. All phones in the hunt group will see a display of 1 call in queue for a few seconds before clearing.

Conditions Call drops only after the 1st round of hunting. If the call is answered in the initial hunting, the call connects. Once the caller is in the queue and hears MOH, if the agent (hunt member) answers the call after that the call will drop.

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 12.4(11)XW3

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XW3

CSCsj97535 BACD functionality broken on freddo

CSCsi50316 Fixed linux builds for RDO tools

CSCsh74385 EEM fails to register with the redundancy framework (RF)

Symptom It is not possible to configure event manager (EEM) applets for redundancyframework (RF) events:

```
nms-7206vxr(config)#event manager applet testapp
nms-7206vxr(config-applet)#event ?
  application  Application specific event
  cli          CLI event
  counter      Counter event
  interface    Interface event
  ioswdsysmon  IOS WDSysMon event
  none         Manually run policy event
  oir          OIR event
  resource     Resource event
  snmp         SNMP event
  syslog       Syslog event
  timer        Timer event
  track        Tracking object event

nms-7206vxr(config-applet)#
```

The keyword for RF is missing as EEM has not registered with RF.

Workaround There is no known workaround.

CSCsj25470 EEM hostnames over 20 characters causes CLI actions to hang

Symptom The Cisco Embedded Event Manager may hang and tie up virtual terminal (vty) lines if the devices host name is longer than 20 characters.

Conditions The device has a hostname configured that is longer than 20 characters. The device has an Embedded Event Manager policy which uses the CLI actions or the CLI TCL library. The Embedded Event Manager policy enters configuration mode using the CLI actions or CLI TCL library.

Workaround Use a hostname less than 20 characters.

Open Caveats - Cisco IOS Release 12.4(11)XW2

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XW2

- CSCsg70474

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

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

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

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

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

- CSCsi60004

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

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

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

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

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

`CSCek78645 Analog phones cannot register with CME`

Symptom Analog phones when configured as SCCP phones cannot register with CCME.

Conditions This happens under any normal conditions. If the phones are configured as SCCP endpoints, the phones will not register.

Workaround There is no workaround.

CSCsj29857 xfer to ICD failed after conference AA

Symptom Occurs when an incoming PSTN call to ICD is routed to an agent and the agent conferences AA. If the agent stays in the conference and tries to transfer the AA to ICD, the call sticks there.

Conditions This happens to the incoming PSTN call when trying to transfer the AA to ICD during conferencing.

Workaround This issue has been resolved. The solution is available in the release of CME (4.2)/12.4(11)XW2.

Open Caveats - Cisco IOS Release 12.4(11)XW1

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)WX1

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

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

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

Cisco 800 series

Cisco 1700 series

Cisco 1800 series

Cisco 2700 series

Cisco 2800 series

Cisco 3700 series

Cisco 3800 series

Workaround For extensive information and a workaround, see the following Field Notice:

http://www.cisco.com/en/US/ts/fn/620/fn62758.html

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

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

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

Workaround There is no workaround. Cisco recommends upgrading to a fixed software release.

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

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

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

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

Symptom

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

Workaround There is no workaround.

Open Caveats - Cisco IOS Release 12.4(11)XW

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release12.4(11)XW

CSCec12299

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

Workarounds are available to help mitigate this vulnerability.

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

This issue cannot be deterministically exploited by an attacker.

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

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

CSCsi01470

A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

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

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

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

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

Workaround Press ENDCALL softkey twice to move the seized DN to idle state after finishing the 2nd trunk call. To work around the one-way audio issue, the call needs to be transferred out and then transferred back. This workaround is not acceptable.

CSCek67866 xcodemsp.c Static Analysis Found Issue

CSCek70830 $$TS: cme crashed during call to ICD routept running 124-11.3.4.PIA1

CSCsg36112 In xcoding, SCCP sessions not cleared immediately after abrupt call end

Symptom When the calls are terminated/disconnected ungracefully or abruptly on an IPIP GW while doing large number of transcoding sessions, some of the sccp and rtp connection of that calls are not cleared immediately on IPIP Gw.

Conditions This happens only when the transcoding calls on IPIP Gw are disconnected abruptly or ungracefully.

Workaround There is no workaround.

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

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

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

Workaround Disable the ip http secure server command.

CSCsg69022 c1700 router crash @ nv_write_internal

Symptom When a user configures the no telephony-service command, router crashes at running configuration generation.

Conditions This symptom is highly unreproducible, but there is a potential race condition between the running configuration generation and the no telephony-service command.

Workaround There is no workaround.

CSCsh65321 Phones fail to do secure authentication in 12.4(12.12)PI6

Symptom Non-7921 phones will not register securely to CME.

Conditions The cnf files for the non-7921 phones have their processNodeName field under CAPF server set to the CAPF IP address. A null value in this field will allow the phones to register securely.

Workaround Remove the processNodeName parameter in the capf server of the phone's cnf file.

CSCsh73754 SmartPorts: PC connected to an IP phone cannot connect to WAN

CSCsh80217 No Audio Path after REFER from xto to xee in a Meetingplace scenario

Symptom No audio heard on Caller IP phone

Conditions Meeting Place RSNA environment

Workaround Yes Fallback image available

CSCsh81876 Traceback & crash if guest mode and multiple vlans

Symptom In case the platform supported number of BSSIDs is 8 then configuring any ssid which comes in the 9th to 16th order in “sh run” as “guest-mode” results in a software crash. In general, if the platform supported BSSIDs considered as X and the maximum supported SSIDs considered as Y then configuring any ssid which comes in the X+1 to Y order(in “sh run”) as “guest-mode” results in crash. Problem is not seen on platforms on which supported number of BSSIDs is 16.

Workaround Configure only that ssid as “guest-mode” which comes in the order 1st to X(platform supported BSSIDs) in “sh run” i.e. if the number of platform supported BSSIDs is 8 then configure any ssid as “guest-mode” which comes in the order 1st to 8th in “sh run”.

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

CSCsi03314 test ecdsa display-stats command not displaying output

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

Symptom A CUCME (Cisco Unified Call Manager Express) router may crash with memory corruption when voice calls are made involving a transcoder.

Conditions Voice calls should invoke a transcoder in order to see this crash.

Workaround None

CSCsi09530 CME SIP phone failed to register because of authenticate register

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

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

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

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

CSCsi15740 Memory leak in basic ICD call

CSCsi22430 B-ACD Crashes CME 4.2

Symptom CME could crash when running B-ACD script while call monitoring is enabled.

Conditions CME could crash if (1) call monitoring is turned AND (2) an incoming call gets routed to any application scripts other than the Default Session.

Workaround The work around is to manually disable callmon before running any non-default applications.

CSCsi27400 Memory leak in TGW for basic SRTP-TLS SIP call

Symptom When a basic SIP call with SRTP using TLS is established between OGW and TGW, a memory leak is observed at the TGW.

Conditions For all inbound calls(RTP/SRTP) where which SRTP and SIPS command is enabled.

Workaround There is no workaround.

CSCsi31667 SIP Registrations sent to Service Provider Proxy for Internal extentions

CSCsi34163 Restore: Radar Detection for non-European regions.

CSCsi42596 router crash when using MeetMe conference with 13 participants

CSCsi44268 $$TS SIP trunk to AA to SIP phone disconnected

Problem Description Call from sip-trunk to CRS/AA sip-phone, call disconnected after 19 seconds.

Symptom The issues observed after V124_11_3_8_PI1A onwards. there was a major ida_t_pi1_atg sync to PI6 occurred in this label.

1. Two reINVITEs sent by originating gateway, received "500 Internal Server Error" on the 2nd reINVITE.
2. Terminating CME does not ACK on the reINVITE(unhold) received.

Root Cause: In **Xfering_SetupDone()** when case of CS_ACTIVE, remove calling AFW_Leg_Resume() again when handling special delayDisconnect call-info in REFER. This code is no longer needed since AFW now unhold the sip XEE before shelbourne hairpin.

Workaround There is no workaround.

CSCsi44465 change CME version from 4.1 to 4.2

Symptom Change CME product version from 4.1 to 4.2

Workaround There is no workaround.

CSCsi44549 Router crashes during pings when QoS+NAT+FW+IPSEC+GRE are configured

CSCsi47359 Crash seen in AFW_Process at the customer site

CSCsi48062 H323--H323--SIP call fails with media transcoder high-density

Symptom On the IPIPGW, an H.323-to-H.323 call fails to complete call setup.

Conditions This problem happens when this call requires transcoding on the IPIPGW and media transcoder high-density is configured for use. Also, after TCS and MSD negotiation, only one of the OGW and TGW sides initiates the OLC negotiation, but not both.

Workaround The workaround is not to use media transcoder high-density on the dial-peers which would handle such described interconnected calls.

CSCsi51441 uclient cannot ping to gateway via non-native vlan

Please refer Release-note enclosure attached to the DDTS CSCsg58791.

CSCsi52410 Add version 6.0 to the available CCM version on dspfarm

CSCsi53006 Router crash in cmm_crs_proc_tr_call_trans_req

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

```
cmm_crs_proc_tr_call_trans_req()
```

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

Workaround There is no workaround.

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

Additional References

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

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.4(11)XW.

- *Cross-Platform Release Notes for Cisco IOS Release 12.4T*
- *Cisco IOS Software Releases 12.4 Special and Early Deployments*
- *Caveats for Cisco IOS Release 12.4(20)T*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 800 series routers are available at http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html

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

Cisco IOS Software Documentation Set

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

Documentation Modules

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