



Release Notes for the Cisco 1800 Series Routers (Fixed) for Cisco IOS Release 12.4(4)XC

March 26, 2008
Cisco IOS Release 12.4(4)XC7
OL-12737-02 Seventh Release
Last Revised: September 24, 2008

These release notes describe new features and significant software components for the Cisco 1800 series routers (fixed) that support Cisco IOS Release 12.4(4)XC. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the [Cross-Platform Release Notes for Cisco IOS Release 12.4T](#) located on [Cisco.com](#).

For a list of applicable software caveats that apply to the Release 12.4(4)XC releases, see the “[Caveats](#)” section on [page 8](#), and see the online [Caveats for Cisco IOS Release 12.4\(4\)T](#) document. The caveats document is updated for every 12.4T maintenance release.

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.

Contents

- [System Requirements, page 2](#)
- [New and Changed Information, page 5](#)
- [Caveats, page 8](#)
- [Additional References, page 50](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 50](#)
- [Open Source License Acknowledgements, page 50](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

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

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 2](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Set Tables, page 3](#)

Memory Requirements

[Table 1](#) lists the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 12.4(4)XC on the Cisco 1800 series routers (fixed).

Table 1 *Memory Requirements for the Cisco 1800 Series Routers (Fixed)*

Platform	Image Name	Image	Flash Recommended ¹	Ram Recommended
Cisco 1801	IP Broadband	c180x-ipbroaband-mz	32 MB	128 MB
	Advanced IP Services	c180x-advipservicesk9-mz	32 MB	128 MB
	Advanced Enterprise Services	c180x-adventerprisek9-mz	32 MB	128 MB
Cisco 1802	Advanced IP Services	c180x-advipservicesk9-mz	32 MB	128 MB
	Advanced Enterprise Services	c180x-adventerprisek9-mz	32 MB	128 MB
Cisco 1803	Advanced IP Services	c180x-advipservicesk9-mz	32 MB	128 MB
Cisco 1811	Advanced IP Services	c181x-advipservicesk9-mz	32 MB	128 MB
	Advanced Enterprise Services	c181x-adventerprisek9-mz	32 MB	128 MB
Cisco 1812	Advanced IP Services	c181x-advipservicesk9-mz	32 MB	128 MB
	Advanced Enterprise Services	c181x-adventerprisek9-mz	32 MB	128 MB

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

Hardware Supported

Cisco IOS Release 12.4(4)XC supports the following routers:

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

For detailed descriptions of new hardware features and which features are supported on each router, see the “[New and Changed Information](#)” section on page 5. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1800 series routers (fixed), which are available on [Cisco.com](#) at the following location:

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

Determining the Software Version

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

```
Router>show version
Cisco IOS Software, C870 Software (C870-ADVENTERPRISEK9-M), Version 12.4(4)XC, EARLY
DEPLOYMENT RELEASE SOFTWARE
Copyright (c) 1986-2006 by Cisco Systems, Inc
```

Upgrading to a New Software Release

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

Feature Set Tables

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



Caution

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

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

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

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

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

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

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

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

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

-
- Step 1** From the Cisco Feature Navigator home page, click **Search by feature**.
 - Step 2** To find a feature, use either “Search by full or partial feature name” or “Browse features in alphabetical order.” Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the Features available text box on the left side of the web page.
 - Step 3** Select a feature from the Features available text box, and click the **Add** button to add a feature to the Features selected text box on the right side of the web page.



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

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

- Step 4** Click **Continue** when you are finished selecting features.
 - Step 5** From the Major Release drop-down menu, choose **12.4**.
 - Step 6** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 7** From the Platform drop-down menu, select the appropriate hardware platform. The “Search Results” table will list all the software images (feature sets) that support the feature(s) that you selected.
-

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

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

-
- Step 1** From the Cisco Feature Navigator home page, click **Compare Images**, and then **Search by Release**.
 - Step 2** In the “Find the features in a specific Cisco IOS release, using one of the following methods:” area, choose **12.4** from the Cisco IOS Major Release drop-down menu.
 - Step 3** Click **Continue**.
 - Step 4** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 5** From the Platform drop-down menu, choose the appropriate hardware platform.
 - Step 6** From the Feature Set drop-down menu, choose the appropriate feature set. The “Search Results” table will list all the features that are supported by the feature set (software image) that you selected.

[Table 2](#) lists the features and feature sets that are supported in Cisco IOS Cisco IOS Release 12.4(4)XC. The table uses the following conventions:

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

**Note**

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

Table 2 Feature List for Cisco 1800 Series Routers

Feature	In	Image
802.1x Basic Authentication	Yes	All. See Table 1 for images
802.1x with Guest VLAN		
802.1x with VLAN Assignment		
Extensible Authentication Protocol		
Cisco Unified CME 4.0(4) Extension Assigner		

New and Changed Information

- [New Features in Cisco IOS Release 12.4\(4\)XC5](#), page 5
- [New Features in Cisco IOS Release 12.4\(4\)XC4](#), page 6
- [New Features in Cisco IOS Release 12.4\(4\)XC3](#), page 6
- [New Features in Cisco IOS Release 12.4\(4\)XC2](#), page 6
- [New Features in Cisco IOS Release 12.4\(4\)XC1](#), page 7
- [New Features in Cisco IOS Release 12.4\(4\)XC](#), page 7
- [New Features in Release 12.4T](#), page 8

New Features in Cisco IOS Release 12.4(4)XC5

- [New Hardware Features in Release 12.4\(4\)XC5](#), page 5
- [New Software Features in Release 12.4\(4\)XC5](#), page 5

New Hardware Features in Release 12.4(4)XC5

There are no new hardware features in this release.

New Software Features in Release 12.4(4)XC5

There are no new software features in this release.

New Features in Cisco IOS Release 12.4(4)XC4

- [New Hardware Features in Release 12.4\(4\)XC4, page 6](#)
- [New Software Features in Release 12.4\(4\)XC4, page 6](#)

New Hardware Features in Release 12.4(4)XC4

There are no new hardware features in this release.

New Software Features in Release 12.4(4)XC4

The following section describes the new software features supported by the Cisco 1800 series routers (fixed) for Cisco IOS Release 12.4(4)XC.

- [Cisco Unified CME 4.0\(4\) Extension Assigner, page 6](#)

Cisco Unified CME 4.0(4) Extension Assigner

The Cisco Unified CallManager Express (CME) feature enables installation technicians to assign extension numbers to Cisco Unified CME phones without accessing the server. For more information, see the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/voice/its/cme40/cme403/extasgnr.html>

New Features in Cisco IOS Release 12.4(4)XC3

- [New Hardware Features in Release 12.4\(4\)XC3, page 6](#)
- [New Software Features in Release 12.4\(4\)XC3, page 6](#)

New Hardware Features in Release 12.4(4)XC3

There are no new hardware features in this release.

New Software Features in Release 12.4(4)XC3

There are no new software features in this release.

New Features in Cisco IOS Release 12.4(4)XC2

- [New Hardware Features in Release 12.4\(4\)XC2, page 6](#)
- [New Software Features in Release 12.4\(4\)XC2, page 7](#)

New Hardware Features in Release 12.4(4)XC2

There are no new hardware features in this release.

New Software Features in Release 12.4(4)XC2

There are no new software features in this release.

New Features in Cisco IOS Release 12.4(4)XC1

- [New Hardware Features in Release 12.4\(4\)XC1, page 7](#)
- [New Software Features in Release 12.4\(4\)XC1, page 7](#)

New Hardware Features in Release 12.4(4)XC1

There are no new hardware features in this release.

New Software Features in Release 12.4(4)XC1

There are no new software features in this release.

New Features in Cisco IOS Release 12.4(4)XC

- [New Hardware Features in Release 12.4\(4\)XC, page 7](#)
- [New Software Features in Release 12.4\(4\)XC, page 7](#)

New Hardware Features in Release 12.4(4)XC

There are no new hardware features in this release.

New Software Features in Release 12.4(4)XC

The following sections describe the new software features supported by the Cisco 1800 series routers (fixed) for Cisco IOS Release 12.4(4)XC:

- [802.1x Basic Authentication, page 7](#)
- [802.1x with Guest VLAN, page 8](#)
- [802.1x with VLAN Assignment, page 8](#)
- [Extensible Authentication Protocol, page 8](#)

802.1x Basic Authentication

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates the first client connected to the port before it opens the port up to the public and making available any services offered by the router or the LAN.

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

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sed/scg/sw8021x.htm#wp1025060>

802.1x with Guest VLAN

When you configure a guest VLAN, clients that are not IEEE 802.1x-capable are put into the guest VLAN when the server does not receive a response to its EAP request/identity frame. Clients that are IEEE 802.1x-capable but that fail authentication are not granted network access. The switch supports guest VLANs in single-host or multiple-host mode.

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

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sed/scg/sw8021x.htm#wp1026004>

802.1x with VLAN Assignment

You can limit network access for certain users by using VLAN assignment. After successful 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the port. The RADIUS server database maintains the username-to-VLAN mappings, which assigns the VLAN based on the user name of the client connected to the port.

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

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sed/scg/sw8021x.htm#wp1062632>

Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) and TLS are both IETF RFC standards. The EAP protocol carries initial authentication information, specifically EAPOL (the encapsulation of EAP over LANs as established by IEEE 802.1x) is an authentication protocol for the 802.1x framework for mutual authentication between the client and a RADIUS server.

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

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacsapp/csapp33/user/sau.htm#wp9

New Features in Release 12.4T

For information regarding the features supported in Cisco IOS Release 12.4T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on [Cisco.com](http://www.cisco.com):

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/xprn124/index.htm>

Caveats

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

Caveats in Cisco IOS Release 12.4(4)T are also in Cisco IOS Release 12.4(4)XC. For information on caveats in Cisco IOS Release 12.4T, see the *Caveats for Cisco IOS Release 12.4(4)T* document. This document lists severity 1 and 2 caveats; the documents are located on [Cisco.com](http://www.cisco.com).

**Note**

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, go to:

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

- [Resolved Caveats - Cisco IOS Release 12.4\(4\)XC7, page 9](#)
- [Open Caveats - Cisco IOS Release 12.4\(4\)XC7, page 15](#)
- [Resolved Caveats - Cisco IOS Release 12.4\(4\)XC6, page 15](#)
- [Open Caveats - Cisco IOS Release 12.4\(4\)XC6, page 22](#)
- [Resolved Caveats - Release 12.4\(4\)XC5, page 22](#)
- [Open Caveats - Release 12.4\(4\)XC5, page 30](#)
- [Resolved Caveats - Release 12.4\(4\)XC4, page 30](#)
- [Open Caveats - Release 12.4\(4\)XC4, page 37](#)
- [Resolved Caveats - Release 12.4\(4\)XC3, page 38](#)
- [Open Caveats - Release 12.4\(4\)XC3, page 38](#)
- [Resolved Caveats - Release 12.4\(4\)XC2, page 38](#)
- [Open Caveats - Release 12.4\(4\)XC2, page 42](#)
- [Resolved Caveats - Release 12.4\(4\)XC1, page 42](#)
- [Open Caveats - Release 12.4\(4\)XC1, page 49](#)
- [Resolved Caveats - Release 12.4\(4\)XC, page 49](#)
- [Open Caveats - Release 12.4\(4\)XC, page 49](#)

Resolved Caveats - Cisco IOS Release 12.4(4)XC7

- CSCec12299

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

Workarounds are available to help mitigate this vulnerability.

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

This issue cannot be deterministically exploited by an attacker.

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

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

- CSCse56501

A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful

exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>

- 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>

- CSCsd81407

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsi80749

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsg70474

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsi60004

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

CSCsg96319 reverse ssh eliminated telnet authentication on VTY

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

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

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_rssh.html

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

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

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

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

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

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

CSCsg03449 Etherswitch module VLAN Trunking Protocol Vulnerabilities

Symptom

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

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

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

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

These vulnerabilities are addressed by Cisco IDs:

- [CSCsd52629/CSCsd34759](#) -- VTP version field DoS
- [CSCse40078/CSCse47765](#) -- Integer Wrap in VTP revision

- [CSCsd34855/CSCei54611](#) -- Buffer Overflow in VTP VLAN name
- [CSCsg03449](#) -- Etherswitch module VLAN Trunking Protocol Vulnerabilities. Cisco's statement and further information are available on the Cisco public website at: <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

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

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

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

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

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

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

Conditions This symptom is seen under the following conditions

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

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

CSCec12299 Corruption of ext communities when receiving over ipv4 EBGP session

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

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

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

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

```
router bgp 1
 address-family ipv4 vrf one
 neighbor 1.0.0.1 remote-as 100
```

```

neighbor 1.0.0.1 activate
neighbor 1.0.0.1 route-map FILTER in
exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
  set extcomm-list 100 delete
!

```

CSCse24889 Malformed SSH version 2 packets may cause processor memory depletion

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

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

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

```

config t

ip ssh version 1
end

```

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

Workaround

```

10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied

```

```

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

```

```

line vty 0 4
access-class 99 in
end

```

Further Problem Description For information about configuring vty access lists, see the [Controlling Access to a Virtual Terminal Line](#) document.

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document: <http://www.cisco.com/warp/public/707/ssh.shtml>

CSCsc40493 Lengthy PADR frame could crash PPPoE BRAS

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

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

Workaround There is no workaround.

CSCsh53643 mbar/isync compiler automation (No RNE available)

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

Open Caveats - Cisco IOS Release 12.4(4)XC7

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(4)XC6

- CSCsf30058

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsb40304

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

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

Cisco IOS is affected by the following vulnerabilities:

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

- Processing Finished messages, documented as Cisco bug ID CSCsd92405

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

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



Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml>.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml>.

CSCsd85587

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

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

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

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

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

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

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



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

<http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml>.

CSCsd92405

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

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

Cisco IOS is affected by the following vulnerabilities:

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

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

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



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

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

CSCek48162: TDM cross connects before last call disconnect and assertions

Symptom : Under heavy stress few tdm assertion failures are seen

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

Workaround: There is no workaround

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

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

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

Workaround : There is no workaround

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

Workaround : See the advisory posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml>

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

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

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

Workaround : There is no workaround.

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

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

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

Workaround : Use process switching

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

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

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

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

CSCse58397: ISDN BRI Dialer Interface is always in up state

Symptom : ISDN B channels are in UP state

Conditions :After reload and after shut/no shut

Workaround : There is no workaround

CSCsf28515: Crashes at mars_default_port_dsp_connect

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

Workaround : There is no workaround

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

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

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

Workaround :There is no workaround

CSCsg16908: IOS FTP Server Deprecation

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

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

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

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

CSCsg47834: NACK is observed for Open Voice Channel command

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

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

Workaround : 1) Disable Trans coding (or)

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

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

```
dspfarm profile 1 trans code
  codec g711ulaw
  codec g729r8
  associate application SCCP
Router(conf-t)#dspfarm profile 1 transcode
Router(config-dspfarm-profile)#maximum sessions 6
```

Example 2:

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

```
dspfarm profile 2 trans code
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  associate application SCCP
Router(conf-t)#dspfarm profile 2 transcode
Router(config-dspfarm-profile)#maximum sessions 8
Use "show voice dsp group all" command to verify DSP resource allocation.
```

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

CSCsg59037: 85x/87x cannot upgrade rommon from IOS

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

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

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

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

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

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

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

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

Conditions : This happens only when trunk DN's are used and they go offhook in quick succession on different phones and are in dialing mode.

Workaround : There is no workaround

CSCsg68711: Incoming call in background does not ring after transfer commit

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

Conditions : While transferring a trunk DN call, a call comes in. After committing the transfer at alert, the incoming call still does not ring on the phone.

Workaround : There is no workaround.

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

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

Conditions : PSTN -- FXO --- CME GATEWAY --- VG224/FXS --- IVR A call comes into a FXO port that is part of a trunk group and gets transferred to an extension that is hanging off of a VG224. DTMF is not relayed to the end point

Workaround : Setting the transfer system to full blind will prevent the DTMF blocking.

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

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

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

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

clock summer-time PDT

recurring 2 Sun Mar 2:00 1 Sun Nov 2:00 (This example is for the US/Pacific time zone.)

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

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

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

Workaround : There is no workaround

Open Caveats - Cisco IOS Release 12.4(4)XC6

There are no open caveats in this release.

Resolved Caveats - Release 12.4(4)XC5

- CSCse56800

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

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

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

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

- CSCsf04754

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

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

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

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmv3.shtml>

- CSCsf11855

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCse05642

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCse68138

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

CSCek26492

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

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

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

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

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

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

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

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

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

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

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

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

Workaround : There is no workaround.

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

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

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

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

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

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

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

Workaround : There is no workaround.

CSCsd47303: Ephone template for ringing state

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

Workaround : There is no workaround.

CSCsd48251: Held call on shared line shows From Unknown Number

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

Workaround : There is no workaround.

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

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

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

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

CSCse05642: I/O memory corruption crash on AS5850

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

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

Workaround : There is no workaround.

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

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

Conditions : The message below is what causes this behavior:

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

Workaround : There is no workaround

CSCse68138: Handle fragmented packets in VOIP RTP Lib

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

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

Workaround : There is no workaround.

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

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

Workaround : There is no workaround.

CSCse82300: Getting Undefined Tone when we enter a invalid FAC

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

Workaround : There is no workaround.

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

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

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

Workaround : There is no workaround.

CSCse87446: Extension assigner defaults provision-tags to 0

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

Workaround : Use the Ephone-tag.

CSCsf02737: Memory Corruption Crash at chunk_free_caller

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

```

abort
crashdump
chunk_free_caller
free_lite_internal
__free
free
skinny_send_msg_internal
skinny_server_process
r4k_process_dispatch

```

Conditions : This seems similar to CSCsb80447.

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

CSCsf07990: CME Dynamic Hunt-Group Login fails

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

```

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

```

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

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

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

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

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

CSCsf21458: SRST Reuses sockets causing phones unregister

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

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

Workaround : There is no workaround.

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

Symptom : The following scenario is seen:

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

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

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

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

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

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

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

Workaround : There is no workaround.

CSCsf99737: SRST Locale fail over soft keys still display English

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

Workaround : There is no workaround.

Open Caveats - Release 12.4(4)XC5

There are no open caveats in this release.

Resolved Caveats - Release 12.4(4)XC4

- CSCse68355

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

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

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

CSCsc74783

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

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

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

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

CSCek47681: Backplane TDM loss and assertion failures

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

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

Workaround : There is no workaround.

CSCse06975: Traceback at pak_copy_contiguous_to_contiguous when testing multicast

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

Workaround : There is no workaround.

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

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

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

Workaround : There is no workaround.

CSCse18940: Memory depletes when VoAAL2 traffic is passed.

Workaround : There is no workaround.

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

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

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

Workaround : There is no workaround.

CSCse47728: Path confirmation failures are observed with VoATM

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

Conditions : This is seen with only with VoAAL2 traffic.

Workaround : There is no workaround.

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

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

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

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

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

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

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

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

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

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

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

Workaround : Disable caller-id on the voice port.

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

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

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

Workaround : There is no workaround.

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

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

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

Workaround : There is no workaround.

CSCse70333: CFwdAll erroneously reconfigured after disabling night service

Symptom : CFwdAll incorrectly appears after night service is disabled.

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

Workaround : Remove CFwdAll via softkey or reload the router.

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

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

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

Workaround : There is no workaround.

CSCse06975: Traceback at pak_copy_contiguous_to_contiguous when testing multicast

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

Workaround : There is no work around.

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

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

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

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

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

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

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

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

Workaround : There is no workaround.

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

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

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

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

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

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

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

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

CSCeh69448: SCCP CME need to clean up TFTP binding.

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

CSCsc82351: Device ID for the Goped phone is incorrect

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

Workaround : There is no workaround.

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

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

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

Workaround : Reset the Cisco IP phone 7931.

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

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

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

Workaround : There is no workaround.

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

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

Workaround : There is no workaround.

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

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

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

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

Conditions : Phone falls back to SRST CME router.

Workaround : There is now workaround.

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

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

CSCse16210: 7920 locale support enhancement.

CSCse29308: CCME extension assigner extra

CSCse35293: CCME extension assigner need to update CNF file.

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

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

CSCse39419: Some phones XML file does not have correct m_vendor

Symptom : Cannot configure the phone through the vendorConfig in the XML file
Further Problem Description: The VendorConfig is missing in the XML file.

Workaround : There is no workaround.

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

Symptom : The console is flooded with MOH error debugs when the MOH source file is unconfigured.

Workaround : There is no workaround.

CSCse65819: Reset needed after extension assignment of 7914 attached phone

Symptom : Using the extension assigner to assign an Ephone will do a simple restart. If that phone has a Cisco IP Phone 7914 attached, the 7914 will not register. A reset is required. The extension assigner should detect the presence of a 7914 and issue a reset instead of a restart for that case.

Conditions : Currently on c3825-adventerprisek9-mz.2006-05-31.GOPED_DEV.

Workaround : There is no workaround.

Open Caveats - Release 12.4(4)XC4

There are no open caveats in this release.

Resolved Caveats - Release 12.4(4)XC3

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

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

Workaround : Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability. See the advisory posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>

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

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

Workaround : There is no workaround.

Open Caveats - Release 12.4(4)XC3

There are no open caveats in this release.

Resolved Caveats - Release 12.4(4)XC2

CSCek24468: Dangling sessions at the end of stress test

Symptom : Dangling bearer channels or voice DSP channels seen after stress test.

Conditions : This is seen under heavy stress with short duration calls.

Workaround : There is no workaround.

CSCek35185: Alignment errors `dsp_stream_mgr_stop_feature`

Symptom : Traceback is observed.

Conditions : Running SS7 stress with COT provisioned.

Workaround : There is no workaround.

CSCek38822: no-reg command does not work on SRST

Symptom : Not able to configure **no-reg** under SRST.

Conditions : Using SRST 3.x or lower

Workaround : There is no workaround.

CSCek40136: The **no-reg** command on Ephone-dn should not apply to dialplan-pattern

Symptom : The dialplan-pattern can not register to SIP proxy or H323 gatekeeper although no **no-reg** configured for it.

Conditions : If **no-reg** is configured for Ephone-dn, its expanded E164 number via dialplan-pattern would not register to a SIP proxy or a H323 gatekeeper.

Workaround : The workaround is to not to configure **no-reg** for Ephone-dn. However, this workaround is not acceptable if the extension is not supposed to be registered.

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

Symptom : An analog or digital CAS port gets into a state where inbound and/or outbound calls coming through the port may not work.

Conditions : This symptom is observed on the Cisco 2800 and Cisco 3800 gateways with analog or digital CAS ports which use PVDM2 DSP modules. When the symptom has occurred, you must reload the gateway to restore proper operation.

Workaround : There is no workaround.

CSCsc46528: Sub entry polling: number of rows returned inconsistently from Speedbird MIB

Symptom : The ccmeEphoneActTable from CISCO-CCME-MIB provides inconsistent results.

Conditions : This symptom occurs when a partial **SNMP GET** is issued on selected columns from a ccmeEphoneActTable.

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

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

Symptom : The index may not come out correctly if performing a **get next** for an item in a table.

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

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

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

Symptom : When a call is put on hold on a 7960 phone and the call was placed on speaker phone mode, resuming the call on another phone does not clear the speakerphone light.

Workaround : Depress the speakerphone light to clear it.

CSCsd14203: MOH play using media play verb does not work

Symptom : BACD AA script crashes while trying to play Music on Hold (MoH)

Conditions : This happens with 12.4 (4) XC and 12.4 (4)T images.

Workaround : Configure Live MoH. Even if you don't have a livefeed source, the script will failover to the MoH file in flash.

The sample below has Ephone-dn config for "dummy" MoH livefeed:

```
Ephone-dn 20 number <dummy-number> moh out-call BCDA! dial-peer voice 7 pots
destination-pattern BCDA!
```

Also enable **debug ephone moh**. Having dummy MoH Livefeed allows the MoH server to get started.

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

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

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

Workaround : Add **progress_ind alert strip** on outgoing dial peer to TGW in OGW. Configure slow start on the GWs. (under voice service VoIP, H.323 mode)

CSCsd35389: Deleted Ephone-dns never unregister with Gatekeeper unless GW reloaded

Symptom : Cisco Unified CallManager Express registers “gatekeeper all” for the Ephone-dn are automatically registered, but when a Ephone-dn is deleted, it never unregisters with the gatekeeper.

Conditions : If you enter the **no gateway** command followed by the gateway command on the CME router to force it to unregister then reregister, the deleted Ephone-dn will show up again.

Workaround : To permanently remove the Ephone-dn reload the CME/gateway or enter the **shut** command followed by the **no shut** command on the gatekeeper.

CSCsd46933: New calls fail at next free DSP channel

Symptom : Under stress with less intercall delay TDM backplane Ds0 may leak on Cisco AS5400XM using a Cisco 5510 DSP.

Conditions : This occurs when incoming and outgoing calls are present and intercall delay is very short.

Workaround : There is no workaround.

CSCsd54232: Qsig Call Forward shows AFW memories leak

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

Workaround : There is no workaround.

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

Symptom : Cisco Unified CallManager Express 4 reloads after the DND button is pressed.

Conditions : When using the Cisco 7970 IP phone with the additional 7914 extension module, pressing the DND button will cause the Call Manager Express to produce tracebacks and reloads.

Workaround : This does not occur when the 7914 is not installed.

CSCsd71195: Path confirmation failed for MGCP calls

Symptom : Path confirmation fails for MGCP calls.

Conditions : This problem occurs when calls are made between NP108 and AS5X-FC feature card.

Workaround : Use the **no voice-fastpath enable** command.

CSCsd78806: Cannot add ATA through GUI

Symptom : While trying to add “ATA” through the GUI for Cisco Unified CallManager Express, an error occurs on page when you try to save the information after configuring the ATA and its not possible to add the ATA.

Conditions : This only applies to “ATA.”

Workaround : Add “ATA” through the command line on the router.

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

Symptom : When a call is being parked from a phone whose primary DN is 8001, it does not get parked to 6101 since we fail to check and match the secondary number of the primary DN.

CSCsd91095: 7936 registration blocked by CLI: no auto-reg-Ephone

Symptom : The command **no auto-reg-Ephone** should not block the 7936 phone from getting registered to Cisco Unified Call Manager Express.

Conditions : This occurs using Cisco IOS version 12.4(4)XC. If **no auto-reg-Ephone** is configured, you are unable to manually register the Ephone associated with the 7936 model.

Workaround Workaround: Enable auto registration using the **auto-reg-Ephone** command

Open Caveats - Release 12.4(4)XC2

There are no open caveats in this release.

Resolved Caveats - Release 12.4(4)XC1

CSCsd02098: SRTP for IOS-H323 is broken in 12.4(5.13)T2 \$TS

Symptom : There is no voice path. Packets are not encrypted or decrypted.

Conditions : The symptom occurs when an SRTP call is made.

Workaround : There is no workaround.

CSCed28266: Software forced crash when adding SIP call headers

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

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

Workaround : There is no workaround.

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

Symptom : To minimize the confusion may occur among customers and TAC, and to make the codebase easy to maintain, this caveat is raised to address the need to make the dot1x configuration applicable to only one layer at any time.

Workaround : the **show dot1x interface <I/F> detail** command is enhanced to include the display of L3 interface dot1x information if the SVI interface is applied.

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

Symptom : This symptom occurs when the voice call fails in the following scenario example:

```
ogw (h323, slow start) -- ipipgw1(sip)---(sip)ipipgw2--tgw(sip)
```

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

Workaround : There is no workaround.

CSCek27525: 802.1x unable to authenticate once VLAN is bridged

Symptom : 802.1x clients are unable to authenticate when the vlan configured for these clients has the dot1x configuration and bridged to BVI interface.

Workaround : There is no workaround.

CSCek27755: Device authorize type for Cisco IP phone does not work.

Symptom : Some 802.1x client options are not authorizing.

Workaround : There is no workaround.

CSCek29149: Flow-around broken with post-sync image to software release

Symptom : With TNP phones, there is no voice-path when flow-around is enabled with the new sync image.

Workaround : There is no workaround.

CSCek32225: VTSP leak seen in SS7 scenario

Symptom : Memory leak seen in VTSP after stress test.

Conditions Conditions: This symptom occurs on the SS7 gateway when a call comes in but doesn't connect, either due to lack of resources or misconfigurations on the other end.

Workaround : There is no workaround.

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

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

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

Workaround : There is no workaround.

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

CSCek34540: **show csm call rate** indicates double the actual rate for incoming CAS

Symptom : The command **show csm call rate** indicate double the actual rate for incoming CAS calls.

Conditions : This symptom occurs with incoming CAS calls.

Workaround : There is no workaround.

CSCek34673: Memory leak after overnight SS7 NI2+ loopback COT stress

Symptom : There is a memory leak in ISDN and VTSP processes.

Conditions : This symptom occurs with long duration stress with SS7 NI2+ and COT provisioned.

Workaround : There is no workaround.

CSCsb23025: Locale installer does not include CME spec phrases

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

Workaround : Use the default locale information.

CSCsb72082: Memory corruption while ending a call

Symptom : A Cisco router acting as a SIP gateway crashes when a call is placed from the SIP phone to a PBX phone.

Workaround : There is no workaround.

CSCsc37763: session_type and chan_type variables of FS OLCs are not updated initially

Symptom : When Fast Start calls are made, the following variables are not updated with the correct values:

```
ccb->h245.olc.chan_type
ccb->h245.olc.session_type
```

Conditions : When Fast Start outbound or inbound calls are made on Cisco GW running 12.3, 12.3T, 12.4 or 12.4T images.

Workaround : There is no workaround.

CSCsc57684: Internal Error and tracebacks on Cisco 5400

Symptom : Internal Errors and tracebacks messages may be seen on 5400 router during normal use.

Workaround : There is no workaround.

CSCsc60509: Memory leak in CCSIP_UDP_SOCKET

Symptom : Low memory is caused by a leak in CCSIP_SPI_UDP.

Conditions : Memory leak occurs if there is a re-Subscribe for a call with a context/out-of-call context subscription. For gateways, this typically will be DTMF subscription.

Workaround : Do not send re-Subscribe/Un-Subscribe.

CSCsc87596: nramp fax fails with DMSP - no route

Symptom : All T.37 on-ramp fax calls fail with a “with DMSP - no route” error.

Conditions : Upon receiving a page of T.4 data from the fax machine, the DocMSP aborts the T.37 onramp session.

Workaround : There is no workaround.

CSCsd16947: Spurious memory access traceback seen from 7914 button smashing

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

Workaround : There is no workaround.

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

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

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

Workaround : There is no work around.

CSCsd36943: CME sends incorrect language code to phone

Symptom : Phone in services mode displays english text when the user-locale is set to Denmark. If the user-locale of the phone is set to Denmark, the phone sends in “dk” as the accepted language in the HTTP headers for IP phone services.

Conditions : Telephony-service user-locale DA.

Workaround : There is no workaround.

CSCsd39342: Call hung when 487 is not received after Cancel

Symptom : Call legs are hung and there is a memory leak in the stack.

Conditions : This symptom occurs when a 487 is not received by the SIP gateway after it sends out a CANCEL message.

Workaround : The remote end must send 487 to CANCEL.

CSCsd46569: Cisco Unified CME delayed call-waiting ring/beep

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

Conditions : this symptom occurs with call-waiting calls on CME. This was initially found in Cisco IOS 12.4(2)T2 on both firmware 7.2(2) and 7.2(4).

Workaround : There is no workaround.

CSCsd47013: 2nd call caller-id not correct with shared lines

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

Conditions : The symptom occurs with two incoming calls on the same shared DN. After the first call is terminated, the second call should be presented for the shared DN on all phones.

Workaround : There is no workaround.

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

Symptom : The Ephone may continually ring.

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

Workaround : Reset the Ephone that has this ringing problem.

CSCsd57802: Voice register CLI is not available for Cisco 2801 adventerprice

Symptom : The **voice register** global command is not accepted.

Conditions : Under **configure terminal**, the **voice register** command is not an option.

Workaround : There is no workaround.

CSCsd58220: Cisco AS5400 does not disconnect call after rxing IDLE

Symptom : The recipients' phone rings continuously even after the caller goes on-hook.

Conditions : When the caller goes on-hook, the gateway receives idle and doesn't recognize the call being IDLE. Therefore, the call does not get disconnected and the recipients' phone continues to ring.

Workaround : The person being called has to pick up the phone for the call to be dropped. No other workaround.

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

Symptom : The Ephone may keep ringing and the display may be incorrect.

Conditions : After several calls made and terminated on the shared DN, the Ephone may suddenly keep ringing with the wrong information shown on the screen.

Workaround : Reset the Ephone or the Cisco Unified CME.

CSCsd60412: SS7 NI2 COT fails with transponder mode in outgoing call with AS5X-FC

Symptom : COT failure when making an outbound voice call in GW.

Conditions : This symptom occurs with an outbound voice call in GW with COT feature enabled in PGW.

Workaround : There is no workaround.

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

Symptom : This symptom occurs with Cisco 7970s and 7971 firmware running on Cisco Unified CME 4.0, the "Acct", "Login", and "Flash" softkeys are wrongly labeled as "No Park", "Service is", and "CallPark".

Conditions : This occurs on Cisco 7970 or 7971 firmware.

Workaround : There is no workaround.

CSCek34759: Based on call ref call_id to be provided in COT REQ to TSP

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

Conditions : This symptom occurs with platforms which use TSP for COT processing

Workaround : There is no workaround.

Open Caveats - Release 12.4(4)XC1

There are no open caveats in this release.

Resolved Caveats - Release 12.4(4)XC

CSCsd28570: **tc1sh** command bypass of AAA authorization commands

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

Conditions : Devices that are not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability. This vulnerability is present in all versions of Cisco IOS that support the **tc1sh** command.

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

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

CSCsd17124: Router crashed due to Illegal Opcode exception

Symptom : The Cisco 1812J router could crash due to one of the following:

- 1) An Illegal Opcode exception.
- 2) An Address error
- 3) A SegV Exception

Conditions : The symptoms have been observed on Cisco 1812-J routers with Cisco IOS Release 12.4(4)T and 12.4(6)T and Common Release 12.3(8r)YH6. The Cisco 180x and 181x routers running with ROMMON version 12.3(8r)YH6 or earlier could also experience this problem.

Workaround : There is no workaround.

Open Caveats - Release 12.4(4)XC

There are no open caveats in this release.

Additional References

Use these release notes with:

Cisco CME:

<http://www.cisco.com/en/US/products/sw/voicesw/ps4625/index.html>

Cisco IP Phones:

<http://www.cisco.com/univercd/cc/td/doc/product/ipcvoice.htm>

Cisco SIP Configuration Guide:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_c/sip_c/sipc1_c/index.htm

Cisco Proxy Server Docs:

<http://www.cisco.com/univercd/cc/td/doc/product/voice/sipproxy/index.htm>

Cisco SRST:

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps2169/product_data_sheet0900aecd805e1e79.html

Cisco 12.4 Voice:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/124tcg/vcl.htm>

Obtaining Documentation, Obtaining Support, and Security Guidelines

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

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

Open Source License Acknowledgements

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

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

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

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

Original SSLeay License:

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

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

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

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".
The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

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

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Use this document in conjunction with the documents listed in the “[Additional References](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

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

© 2007, Cisco Systems, Inc. All rights reserved.

