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

March 26, 2008
Cisco IOS Release 12.4(11)XV1
OL-13104-03 Second Release

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

For a list of the software caveats that apply to the Release 12.4(11)XV releases**,** see the "Caveats" section on page 7, and see the online *Caveats for Cisco IOS Release 12.4(4)T* document. The caveats document is updated for every 12.4T maintenance release and is located on Cisco.com.

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/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

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

System Requirements

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

Memory Requirements

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

Table 1 Memory Requirements for the Cisco 1800 Series Routers

Platform	Image Name	Image	Flash (MB)	Ram (MB)
Cisco 1841	Cisco 1841 IOS Advanced Enterprise Services Cisco 1841 IOS AISK9-AESK9 Feature Set Factory UPG For Bundles Cisco 1841 IOS ASK9-AESK9 Feature Set Factory UPG For Bundles Cisco 1841 IOS BB-AESK9 Feature Set Factory UPG For Bundles	c1841-adventerprisek9-mz	64	192
	Cisco 1841 IOS Advanced IP Services Cisco 1841 IOS ASK9-AISK9 Feature Set Factory UPG For Bundles Cisco 1841 IOS BB-AISK9 Feature Set Factory UPG For Bundles Cisco 1841 IOS AISK9-AISK9 Feature Set Factory UPG For Bundles	c1841-advipservicesk9-mz	64	192

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

Hardware Supported

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

- Cisco 1841

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

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

Determining the Software Version

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

```
Router>show version
Cisco IOS Software, C1800 Software (C1800-ADVENTERPRISEK9-M), Version 12.4(11)XV, EARLY
DEPLOYMENT RELEASE SOFTWARE
Copyright (c) 1986-2007 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 Release 12.4(11)XV.

The table uses the following conventions:

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

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

Table 2 Cisco IOS Release 12.4(11)XV Feature List for Cisco 2800 Routers

Feature	In	Image
3G Wireless High-Speed WAN Interface Card	12.4(11)XV	See Table 1 for image names.

New and Changed Information

This section contains the following information:

New Hardware Features in Release 12.4(11)XV1

There are no new hardware features in this release.

New Software Features in Release 12.4(11)XV1

There are no new software features in this release.

New Hardware Features in Release 12.4(11)XV

3G Wireless High-Speed WAN Interface Card

The Third Generation (3G) Wireless High-Speed WAN interface card (HWIC) is a multiband, multiservice WAN card. The primary application of 3GHWIC is WAN connectivity as a backup datalink for critical data applications. The 3G wireless WAN HWIC can also function as the primary WAN connection. The 3G HWIC supports the following Cisco integrated services routers (Cisco ISRs):

- Cisco 1841

The 3G wireless WAN HWIC provides broadband WAN connectivity using high speed cellular data technology and it supports the following GSM and CDMA technologies:

- High-speed Downlink Packet Access (HSDPA)
- Universal Mobile Telecommunications System (UMTS)
- Enhanced Data-Rates for GSM Evolution (EDGE)
- General Packet Radio Service (GPRS)
- Evolution-Data Optimized (EVDO)
- 1 times Radio Transmission Technology (1xRTT)
- Automatic best network selection
- Multiple external antenna options
- Static and dynamic IP addressing
- Modem-based support for mobile IP
- Cellular interface based on the async interface in Cisco IOS
- NAT support
- Security features like Firewall, IDS/IPS and IPSec VPN on the router
- WAN switchover using IOS backup interface feature

New Software Features in Release 12.4(11)XV

There are no new software features for this release.

New Features in Release 12.4T

For information regarding the features supported in Cisco IOS Release 12.4T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on 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 Release 12.4(11)XV. For information on caveats in Cisco IOS Release 12.4T, see the *Caveats for Cisco IOS Release 12.4(4)T* document. This document lists severity 1 and 2 caveats; the documents are located on Cisco.com.

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

Caveats for Cisco IOS Release 12.4(11)XV

Open Caveats - Cisco IOS Release 12.4(11)XV1

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(11)XV1

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.

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

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

`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.

`CSCsi56163 SIM read failure on bootup for certain SIMs causes Unknown SIM status`

Symptom Certain SIMs on certain GSM HWICs exhibit read failure causing SIM Unknown status.

Conditions Router bootup with the affected SIMs

Workaround Use a valid working service provider approved SIM.

`CSCsi72340 C1841 crashed while upgrading GSM firmware`

Symptom Router crash with memory corruption while attempting firmware upgrade on HWIC-3G-CDMA or HWIC-3G-GSM

Conditions The trigger is firmware upgrade process for HWIC-3G-GSM or HWIC-3G-CDMA.

Workaround There is no workaround

CSCek66393FPM: router crashes with large size buffer

CSCsi95130 Router crashes while activating the modem if wrong params are used

Symptom Router crash while trying to enter "cellular x/y/z activate manual command.

Conditions While activating a modem on a HWIC-3G-CDMA using “manual activation” method, if activation code is entered that has either “*” or”#”, then the router can crash. The last parameter for activating the modem is Mobile Subscriber Lock (MSL). This is a six digit code. The CLI allows the user to enter a digit [0-9] or *or #. However if * or # is entered as MSL code, then the router can crash while processing this command.

Workaround There is no workaround. Although this will happen only if wrong parameters are entered. The command works w/o any problem for normal operation.

Further Problem Description: “cdma activate manual” command needs to be used only once while trying to activate the CDMA service.

Following params are required for that MDN - 10 digit phone number. MSID - 10 digit mobile Mobile ID

MSL - 6 digit activation code SID - System ID

NID - Network ID

MDN/MSID/MSL are given out by the service provider.

SID/NID is obtained by issueing show cellular network command.

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

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

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

Workaround There is no workaround.

CSCsj06951 Traceback @ createCNF_file while configuring user-locale

Symptom Traceback seen on terminal.

Conditions When config user-locale and generate CNF file under telephony-service.

Workaround There is no workaround

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

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

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

Cisco 800 series

Cisco 1700 series

Cisco 1800 series

Cisco 2700 series

Cisco 2800 series

Cisco 3700 series

Cisco 3800 series

Workaround For extensive information and a workaround, see the following

Field Notice:
http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

CSCsj16172 WIC-1SHDSL-V3 blocks data. Error in check_tx_ready: VCD not in use

Symptom In a back to back setup WIC-1SHDSL-V3 fails to pass traffic. Each time PPP sends a frame the debugs report:

00:00:47.707: ATM0/1/0: Error in check_tx_ready: VCD not in use, vcd: 1

00:00:49.723: ATM0/1/0: Error in check_tx_ready: VCD not in use, vcd: 1

00:00:51.739: ATM0/1/0: Error in check_tx_ready: VCD not in use, vcd: 1

00:00:53.755: ATM0/1/0: Error in check_tx_ready: VCD not in use, vcd: 1

Conditions The problem is seen with 12.4(11)XV release

Workaround Use either a mainline or a T-train release

CSCsg15598 DYIDS: Fragmentation prevents signature recognition

The Intrusion Prevention System (IPS) feature set of Cisco IOS® contains several vulnerabilities. These include:

- Fragmented IP packets may be used to evade signature inspection.
- IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at:

http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml

CSCsh58082 SIP: A router may reload due to SIP traffic

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

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

CSCec12299 Corruption of ext communities when receiving over ipv4 EBGP session

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

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

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

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

```
router bgp 1
 address-family ipv4 vrf one
 neighbor 1.0.0.1 remote-as 100
 neighbor 1.0.0.1 activate
 neighbor 1.0.0.1 route-map FILTER in
 exit-address-family
!
ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
 set extcomm-list 100 delete
!
```

CSCsj18014 Caller ID string received with extra characters

Symptom A caller ID may be received with extra characters. Conditions: This symptom is observed when caller ID is enabled on both routers and when the station ID and station name are configured on the FXS side.

Workaround There is no workaround

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

%SYS-3-TIMERNEG errors and tracebacks are observed while making MGCP RSVP calls on a analog (RGW) setups. Observed in 12.4(3.9)T1 IOS version.

Workaround There is no workaround.

CSCsj16292 DATACORRUPTION-1-DATAINCONSISTENCY: copy error

Symptom Following an upgrade to Cisco IOS Release 12.2(18)SXF9, the following message may be displayed:

%DATACORRUPTION-1-DATAINCONSISTENCY: copy error-Traceback=

Conditions This message may appear as a result of SNMP polling of PAgP variables, but does not appear to be service impacting.

Workaround There is no workaround.

CSCsj13380 Possible problem with calling numbers when called_num_chunk not nulled

Symptom Data corruption messages may be displayed, and show isdn active may show incorrect information for calling number on outgoing calls. This problem is inconsistant, and shows up most frequently with the “isdn test call” CLI.

Conditions Outbound calls.

Workaround There is no workaround.

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.

CSCse24889 Malformed SSH version 2 packets may cause processor memory depletion

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

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

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

config t

ip ssh version 1

end

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

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

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

line vty 0 4
access-class 99 in
end
```

Further Problem Description: For information about configuring vty access lists, see the *Controlling Access to a Virtual Terminal Line* document:

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

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

CSCdz55178 QoS profile name of more then 32 chars will crash the router

Symptom A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

Conditions This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                         00000000011111111111222222222333^
                         12345678901234567890123456789012|
                                                          |
                                                   PROBLEM
                                                 (Variable Overflowed).
```

Workaround Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

CSCsd58772 rttMonLatestRttOperTime is always 0 for RTP Probe.

Symptom The MIB object rttMonLatestRttOperTime returns a value of 0.

Conditions This symptom occurs for IPSLA RTP operation only irrespective of whether the operation succeeds or fails.

Workaround There is no workaround

CSCsj52927 DATACORRUPTION-1-DATAINCONSISTENCY message in show log

Symptom DATACORRUPTION-1-DATAINCONSISTENCY messages are seen in 'show log'

Conditions The messages are seen when when the router comes up.

Workaround There is no workaround.

CSCsj32707 GW rejects SIP UPDATE with Cseq 0

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

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

Workaround There is no workaround. Note that the symptom does not occur in Release 12.4(9)T3.

CSCec12299

Symptom 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.

Conditions 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.

Workaround 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.

Open Caveats - Cisco IOS Release 12.4(11)XV

CSCsh40495 On HWIC-3G-GSM and in rare occasions EDGE/GPRS Rx data traffic stops until reset the modem

Further Problem Description: In rare occasions it has been observed that the modem may get into a state where the Rx (Inbound from the Wireless Network to Device) path is blocked. This problem has only been observed when the modem is attached to EDGE service and after a few hours of operation. A modem reset is required to come out of this state.

Workaround As this problem is related to the signal quality at a given location, repositioning the antenna could potentially solve this problem. Using the 20ft or 50ft Cable options, the antenna can be moved out of the spot where interference from multiple cells causes the modem Rx path failure.

When using an attached antenna, relocating the router to a location away from the problem spot can eliminate the problem.

When the failure occurs, a modem reset using the following IOS command would bring the modem out of failure state:

```
test cellular x/x/x modem-reset
```

CSCse92662:HWIC data path stops working

Symptom :HWIC data path stops working under stress condition. Both transmit and receive directions will be impacted. The problem is not specific to any particular cellular technology

Conditions : Stress over long period of time.

Workaround Reload the router

Resolved Caveats - Cisco IOS Release 12.4(11)XV

CSCsf08998

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

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

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

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

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

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.

Additional References

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

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

- Release-Specific Documents, page 19
- Platform-Specific Documents, page 19

Release-Specific Documents

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

- *Cross-Platform Release Notes for Cisco IOS Release 12.4(11)T*
- *Field Notices:* http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- Caveats for Cisco IOS Release 12.4 and *Caveats for Cisco IOS Release 12.4(11)T*

Platform-Specific Documents

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

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

Cisco IOS Software Documentation Set

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

Documentation Modules

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

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

References

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/callc_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/products/sw/voicesw/ps2169/index.html

Cisco 12.4 Voice:

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

Open Source License Acknowledgements

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

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

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

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN

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

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

Original SSLeay License:

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

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

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

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].

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.htmlCisco.com

---

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