Release Notes for Cisco 3200 Series Routers for Cisco IOS Release 12.4(6)XE

March 26, 2008
Cisco IOS Release 12.4(6)XE3
OL-10693-02 Third Release

These release notes describe new features and significant software components for Cisco 3200 series routers in Cisco IOS Release12.4(6)XE releases. 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 in PDF or HTML format.

For a list of the software caveats that apply to Cisco IOS Release12.4(6)XE releases**,** see the "Caveats" section on page 6, and see the online *Caveats for Cisco IOS Release 12.4T* 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 system requirements for Cisco IOS Release 12.4(6)XE and includes the following sections:

Memory Requirements

Table 1 lists memory requirements for Cisco IOS feature sets supported by Cisco IOS Release 12.4(6)XE on Cisco 3200 series routers.

Table 1 Memory Requirements for Cisco 3200 Series Routers

Platform	Feature Set	Image	Flash Memory[1]	RAM Memory
Cisco 3220	Advanced Enterprise	c3220-adventerprisek9-mz	32 MB	128 MB
Cisco 3250	Enterprise Base	c3250-entbase-mz	32 MB	128 MB
Cisco 3250	Advanced Enterprise	c3250-adventerprisek9-mz	32 MB	128 MB
Cisco 3270	Enterprise Base	c3270-entbase-mz	64 MB	256 MB
Cisco 3270	Advanced Enterprise	c3270-adventerprisek9-mz	64 MB	256 MB

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

Hardware Supported

Cisco IOS Release 12.4(6)XE supports the following Cisco 3200 series routers:

- Cisco 3220 router
- Cisco 3250 router
- Cisco 3270 router

For descriptions of existing hardware features and supported modules, see the configuration guides and additional documents specific to Cisco 3200 series routers, which are available on Cisco.com at the following location:

http://www.cisco.com/en/US/products/hw/routers/ps272/tsd_products_support_series_home.html

or point your web browser to Cisco.com and follow this path:

Technical Support & Documentation: **Documentation**:**Routers: Cisco 3200 Series Wireless and Mobile Routers**

Determining the Software Version

To determine which version of Cisco IOS software is currently running on your Cisco 3200 series router, 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
c3270-perf#sh ver
Cisco IOS Software, C3270 Software (C3270-ADVENTERPRISEK9-M), Experimental Version
Synched to technology version 12.46)XE
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 consisting of software images, which vary with the platform. Each feature set contains a specific set of Cisco IOS features. Cisco IOS Release 12.4(6)XE supports the same feature sets as Cisco IOS Release 12.4T, as well as new features.

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

Table 2 on page 3 lists new features and feature sets in Cisco IOS Release 12.4(6)XE.

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 The feature set table contain only a selected list of features, which are cumulative for Release 12.4(6)*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 12.4T* documentation.

Table 2 New Feature List for Cisco 3200 Series Routers

Feature	In	Image
Cisco 3270 Rugged Router	Yes	All. See Table 1 for images.
Mobile Networks NAT Traversal		

New and Changed Information

The following sections describe new features supported by Cisco 3200 series routers in Cisco IOS Release 12.4(6)XE.

New Hardware Features in Cisco IOS Release 12.4(6)XE

The following section describes new hardware features for Cisco 3200 series routers in Cisco IOS Release 12.4(6)XE.

Cisco 3270 Rugged Router

The Cisco 3270 rugged router is a high-performance rugged processor card designed to support multiple applications running concurrently over wired or wireless networks. With on-board hardware encryption, the Cisco 3270 rugged router offloads encryption processing from the router CPU to provide secure, yet scalable, video, voice, and data services for outdoor and mobile networks.

The Cisco 3270 rugged router allows for a greater number of peripheral devices to be connected, including a broader selection of network interfaces such as fiber, gigabit Ethernet copper, and USB. The Cisco 3270 rugged router is capable of supporting two stacks of PC-104+ mobile interface cards (MICs). With higher performance, increased port densities, and greater network module expansion, the Cisco 3270 delivers investment protection for customers deploying embedded outdoor and mobile networks.

The Cisco 3270 rugged router is offered as a standalone (spare) router card or as a bundle of cards assembled in a rugged enclosure.

Note These release notes are intended for the system administrator (SA), system integrator (SI), and system engineer (SE), who are experts with networking industry training and experience. We assume that users are familiar with the terminology and concepts of the PC-104, Cisco IOS, and mobile IP networking.

For more information about Cisco 3200 series routers, see the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps272/tsd_products_support_series_home.html

New Software Features in Cisco IOS Release 12.4(6)XE

The following sections describe new software features supported on Cisco 3200 series routers in Cisco IOS Release12.4(6)XE.

Mobile IP Support for NAT Traversal

The mobile IP support for RFC 3519 NAT traversal on the Cisco 3200 series router feature extends support for Network Address Translation (NAT) traversal to the mobile router in the scenario in which there is no foreign agent and the mobile router needs to register to the home agent directly using a private collocated care-of address (CCOA).

NAT traversal is based on the RFC 3519 specification and defines how mobile IP should operate to traverse networks that deploy NAT within their network. NAT traversal allows mobile IP to interoperate with networks that have NAT enabled, by providing an alternative method for tunneling mobile IP data traffic. New extensions in the mobile IP registration request and reply messages have been added that establish User Datagram Protocol (UDP) tunneling.

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

http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/software/ios124/124newft/124t/124t_105/htmipmar.htm#wp1049404

Modified CLI Command

The **service declassify** command has been modified with this release.

To enable the declassification function to monitor the trigger signals from the declassification trigger, use the **service declassify** command in global configuration mode. To disable the declassification function, use the **no** form of this command.

service declassify [erase-default |erase-flash | erase-nvram | erase-all] [trigger AUX | GPIO]

no service declassify [erase-default |erase-flash | erase-nvram | erase-all] [trigger AUX | GPIO]

The following options have been added to the service declassify command:

- **trigger**, **AUX**, and **GPIO** (General Purpose Input Output)
  - The **trigger** option enables the declassification trigger source.
  - The **AUX** option enables the declassification trigger on the AUX port CTS pin. This is the default trigger source.
  - The **GPIO** option enables the declassification trigger on the actuator.

  The trigger option is supported on customized Cisco 3270 router boards only. The system integrator needs to install a special cable or actuator so the GPIO trigger source can be used on the customized boards. For Cisco 3270 routers with standard enclosures, the trigger option does not need to be configured.

  After declassification is enabled and the AUX port is selected as the trigger source, the AUX port on the router should not be used for any other functions, or the router may receive false trigger signals. On certain customized Cisco 3270 routers, you can enable declassification and select the special actuator connecting the GPIO port as the trigger source. In this case, the AUX port can still be used for regular data functions.

New Software Features in Cisco IOS Release 12.4T

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

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

or point your web browser to Cisco.com and follow this path:

Technical Support & Documentation: Documentation: Cisco IOS Software: Cisco IOS Software Releases 12.4 T

Limitations and Restrictions

USB Storage Limitation—When a USB Flash storage device is plugged into port 1 and is active while a second USB Flash storage device is plugged into port 2, an error may occur on the active port 1 device.

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(6)T are also in Release 12.4(6)XE. For information on caveats in Cisco IOS Release 12.4T, see the *Caveats for Cisco IOS Release 12.4T* 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 click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4 > Troubleshooting > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section contains the following caveat information:

Resolved Caveats - Cisco IOS Release 12.4(6)XE4

CSCsv04836

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

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

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

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

Resolved Caveats - Cisco IOS Release 12.4(6)XE3

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.

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: http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter

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

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.

CSCsd92405 router crashed by repeated SSL connection with malformed finished message

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.

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.

CSCsd85587 7200 Router crashes with ISAKMP Codenomicon test suite

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 CSCsi97695

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 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

`CSCse83555  Cisco IOS pauses indefinitely with a malformed ISAKMP message`

Symptom Cisco IOS pauses indefinitely or reloads unexpectedly with malformed ISAKMP messages.

Conditions This problem affects the following IOS releases:

- 12.4(8), 12.4(8a), and 12.4(8b)
- 12.4(9)T, and 12.4(9)T1
- 12.4(6)XE and 12.4(6)XE1
- 12.4(9)MR
- 12.4(9)XG

The IOS device must be configured to process IKE messages (which is the default), and must receive a malformed IKE message from a peer with valid credentials.

Workaround There are no workarounds.

Further Information: The crash occurs in Quick Mode which means that phase 1 must have been completed, which requires knowledge of the pre-shared key or having a valid certificate (depending on IKE phase 1 configuration.)

`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:

- CSCsd34759 -- VTP version field DoS
- CSCse47765 -- Integer Wrap in VTP revision
- 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

`CSCsh58082  SIP: A router may reload due to SIP traffic`

Symptom Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP.

There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

Workaround Workarounds exist to mitigate the effects of this problem on devices which do not require SIP.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

`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

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.

CSCsg16908 IOS FTP Server Deprecation

Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's file system, including the device's saved configuration, which may include passwords or other sensitive information.

The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the IOS FTP Client feature.

This advisory is posted at

http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

CSCsi84017 c2600 router hangs during reload

Symptom When you reload a Cisco 2600 series, the router may hang.

Conditions This symptom is observed on a Cisco 2600 series when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

Workaround There is no workaround.

CSCsi09530 CME SIP phone failed to register because of authenticate register

Symptom If the **authenticate register** command is configured under the **voice register global** command, CME SIP failed to registered.

Conditions The **authenticate register** command is configured under the **voice register global** command when CME is acting as a registrar.

Workaround Disable the **authenticate register** command under the **voice register global** command.

Further Problem Description: In registrar functionality, CME challenges an inbound register request with a 401 response. If the **authenticate register** command is configured under the **voice register global** command, the Registering Endpoint then ends a Register Request with Credentials. The Gateway Stack is not processing this request and is dropping it.

CSCsf07847 cdp may fail to discover neighbor information in releases with CSCse85200

Symptom Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

Conditions This issue occurs in IOS images that has the fix for CSCse85200.

Workaround Disable CDP on interfaces where CDP is not required.

Further Problem Description: Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

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 rejaected 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.

CSCsj44081 Improvements in diagnostics and instrumentation

Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS Software releases published after April 5, 2007.

Details: With the new enhancement in place, IOS will emit a %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp

```
May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

The error message is then followed by a traceback.

It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

Recommended Action Collect "show tech-support" command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the %DATACORRUPTION-1-DATAINCONSISTENCY message and note those to your support contact.

- CSCsh53643 mbar/isync compiler automation
- CSCsh77241 Reverting the compliler back to c2.95.3-plib
- CSCsh75069 Input Queue Wedge with UDP Echo packets

- CSCsh87705 GCC compiler modifications
- CSCsh87711
- CSCsh87715
- CSCsh23148 c32xx MMU mapping refinements
- CSCek56536 memory leak under simpleudpfuzz attack for port 500
- CSCsh15703 c815 and c1700 MMU mapping refinement
- CSCsh20392 vg200 and c2600 MMU mapping refinements
- CSCsh46705 Remove unused func declaration of vtsp_tsp_call_disconnect_ind_rawsignal
- CSCek66935 migrate autobahn76 to c2.95.3-p11c compiler
- CSCej53426 miata6 gcc.c3.4.3 rollout: compiler versioning infrastructure

Resolved Caveats - Cisco IOS Release 12.4(6)XE2

`CSCsf04754: Two authentication vulnerabilities in SNMPv3 feature`

Symptom 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.

Workaround 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-snmpv3.shtml

`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 workaround.

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.

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.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload the gateway to restore proper operation.

Further Problem Description: The changes in CSCse15025 includes changes in CSCsc11833 and CScsd90851. These changes have been shown to help mitigate this problem in the majority of cases.

There is a further detection and reset mechanism in CSCse15025 that will recover the DSP which is in this state. This mechanism will trigger immediately if the impacted voice port is an analog FXO port. For other voice ports, a delay in the detection will be present and it is possible to see the symptom of this problem before the recovery code triggers.

Note that the reset mechanism will cause any active calls utilizing the DSP in question to be dropped. It is recommended if running with modules which can be impacted by this issue to upgrade to a release of software which contains the changes in CSCse15025.

If the DSP is reset and the below output is seen, contact the TAC for further assistance. Note that this output is sent at debug level and it is recommended to enable either syslog or logging buffered on the gateway.

Logging buffered on the gateway is enabled through the global command logging buffered 50000 debug as an example to set the logging buffered to use 50K bytes of processor memory for logging. The output of the log can be seen with the exec command **show log**.

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

Symptom One-way voice.

Conditions Ephones A, B, and C are on 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.

CSCse29031: H323-H323 slow start flow around support on IPIPGW in H245 passthru mode

Symptom No support for media flow-around in h245 passthru mode.

Workaround There is no workaround.

CSCse47728: Path confirmation failures with VoAAL2 traffic

Symptom Path confirmation failures seen with Voice over ATM traffic.

Workaround There is no workaround.

CSCse60762: Traceback seen at gk_endpt_global_queue_remove

Symptom Traceback seen on the gatekeeper while deleting **endpoint max-calls** CLI.

Workaround There is no workaround.

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

Symptom When trying to configure **call-waiting ring** on a **ephone-dn x**, the configuration is accepted, but cannot be seen in the configuration in show running.

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 Its 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.

CSCse72236: OLC carried ipipgw ip address in flow-around mode for h323-h323 ss call

Symptom In H323-H323 Slow Start Flow-around mode. OLC and OLC ACK should carried the remote's ip address and media port info. But on haw_t, ipipgw's ip address is used in one of the OLC message toward to the remote GW. This is not correct.

Conditions The flow-around call is still OK since the OLC ACK carried the correct info.

Workaround There is no workaround.

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

Symptom CME/SRST Not able to make calls to Unity VM.VM port DN is not coming to “Idle” state after restarting Unity.

Workaround There is no workaround.

CSCse96018: Three-party conference fails to continue

Symptom Analog phones connected to the Cisco VG224 voice gateway can establish a three-party conference. After establishing the three-party conference, it is not sustained, the Cisco VG224 phone is fed with re-order tone.

Conditions This has been seen when the other two parties of the three-party conference are SIP IP phones.

Workaround There is no workaround.

Resolved Caveats - Cisco IOS Release 12.4(6)XE1

CSCek39526: Router crashed @ tagsw_tfib_rewrite_print when show ipv6 cef int

CSCek45222: QOS service-policy commaand no longer available for vlan interface

CSCek45370: Ping fail from Ipanema FIO PRI interface

CSCse56129: VG224 erroneously triggers hookflash during CME call pickup interaction

CSCse59347: Cme/srst ip phone unregister does not down the virtual POTS peers

CSCse68355: Router crashed by single SIP invite packet

Special Caveats and Updates

SIP Bugs in 12.4(6)XE

- CSCeb21064

  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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

  Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

  Cisco Unified MeetingPlace XSS Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

- CSCej20505

  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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

  Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

  Cisco Unified MeetingPlace XSS Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

- CSCsb24007

  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

Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

Cisco IOS Information Leakage Using IPv6 Routing Header

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

Cisco IOS Next Hop Resolution Protocol Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Cisco IOS Secure Copy Authorization Bypass Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

- CSCsc60249

  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

Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

Cisco IOS Information Leakage Using IPv6 Routing Header

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

Cisco IOS Next Hop Resolution Protocol Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Cisco IOS Secure Copy Authorization Bypass Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

  Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

  Cisco Unified MeetingPlace XSS Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

- CSCse40276

  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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

  Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

  Cisco Unified MeetingPlace XSS Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.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

Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

Cisco IOS Information Leakage Using IPv6 Routing Header

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

Cisco IOS Next Hop Resolution Protocol Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Cisco IOS Secure Copy Authorization Bypass Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

- 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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

- CSCsf08998

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

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

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

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

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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

  Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

  Cisco Unified MeetingPlace XSS Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.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

Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

Cisco IOS Information Leakage Using IPv6 Routing Header

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

Cisco IOS Next Hop Resolution Protocol Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Cisco IOS Secure Copy Authorization Bypass Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

- 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

Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

Cisco IOS Information Leakage Using IPv6 Routing Header

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

Cisco IOS Next Hop Resolution Protocol Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Cisco IOS Secure Copy Authorization Bypass Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.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

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

  Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

  Cisco Unified MeetingPlace XSS Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.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

Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

Cisco IOS Information Leakage Using IPv6 Routing Header

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

Cisco IOS Next Hop Resolution Protocol Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Cisco IOS Secure Copy Authorization Bypass Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

NHRP Bugs in IP Routing Protocols

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

Cisco IOS Information Leakage Using IPv6 Routing Header

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

Cisco IOS Next Hop Resolution Protocol Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

Cisco IOS Secure Copy Authorization Bypass Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

- http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

SCP Bugs in 12.4(6)XE

- CSCsc19259

  The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml.

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  - http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

  Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

Cisco Unified MeetingPlace XSS Vulnerability

– http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

IPv6 Bugs in 12.4(6)XE

- CSCef77013

  Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

  Cisco has made free software available to address this vulnerability for affected customers. 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-20070808-IOS-IPv6-leak.shtml.

  Please Note: The August 08, 2007 publication includes four Security Advisories and one Security Response. The Advisories all affect Cisco IOS, one additionally affects CuCM as well. Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities for all four Cisco IOS issues. Individual publication links are listed below:

  Cisco IOS Information Leakage Using IPv6 Routing Header

  – http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-swap.shtml

  Cisco IOS Next Hop Resolution Protocol Vulnerability

  – http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

  Cisco IOS Secure Copy Authorization Bypass Vulnerability

  – http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml

  Voice Vulnerabilities in Cisco IOS and Cisco Unified Call Manager

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

  Cisco Unified MeetingPlace XSS Vulnerability

  – http://www.cisco.com/warp/public/707/cisco-sr-20070808-mp.shtml

Additional References

The following sections describe the documentation available for the Cisco 3200 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 as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com in pdf or html form.

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

- Release-Specific Documents, page 32
- Platform-Specific Documents, page 32

Release-Specific Documents

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

- *Cross-Platform Release Notes for Cisco IOS Release 12.4(11)T*
- *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 3200 series routers are available on Cisco.com at the following location:

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

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.4 and Cisco IOS Release 12.4(6)XE, and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only.

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Cisco Feature Navigator is available 24 hours a day, 7 days a week.

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

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

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

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

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 (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].

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