Release Notes for the Cisco Mobile Wireless Home Agent Feature in Cisco IOS Release 12.4(22)YD

Published: February 11, 2009

Revised: November 27, 2009, OL-21441-01

Cisco IOS Release 12.4(22)YD is a special release that is based on Cisco IOS Release12.4, with the addition of enhancements to the Cisco Mobile Wireless Home Agent (HA) feature. The Cisco IOS Release 12.4(22)YD is a release optimized for the Cisco Mobile Wireless Home Agent feature on the Cisco Service Application Module for IP (SAMI) for the Cisco 7600 Series. The physical interfaces supported on the Cisco 7600 Series platforms are mainly Fast Ethernet and Gigabit Ethernet, FlexWAN (ATM, Frame Relay), and the new line of Shared Port Adaptor (SPA) and SPA Interface Processor (SIP) line cards, and are independent of physical media.

Contents

These release notes include important information and caveats for the Cisco Home Agent software feature provided in Cisco IOS 12.4(22)YD for the SAMI card on the Cisco 7600 Internet Router platform.

Caveats for Cisco IOS Release 12.4 can be found on Cisco.com at:

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

Release notes for the Cisco 7600 Router can be found on Cisco.com at:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_release_notes_list.html

This release note includes the following topics:

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

Introduction

The Cisco Mobile Wireless Home Agent serves as an anchor point for subscribers, providing easy, secure roaming with quality of service (QoS) capabilities to optimize the mobile user experience. The Cisco Mobile Wireless Home Agent (HA) works in conjunction with a Foreign Agent (FA) and mobile node to provide an efficient Mobile IP solution.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(22)YD:

Memory Requirements

Table 1 shows the memory requirements for the Home Agent Software Feature Set that supports the SAMI blade on the Cisco 7600 Internet router platform.

Table 1 Memory Requirements for the SAMI on the Cisco 7600 Router Platform

Platform	Software Feature Set	Image Name	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7600 Internet Router	HA Software Feature Set	SUP32, SUP720 and RSP720 HA Image 12.4(22)YD	256MB	2GB 1GB DRAM	RAM

Hardware Supported

For platform details and complete list of interfaces supported on 7600 series router, please refer to the following URL on Cisco.com:
http://www.cisco.com/en/US/products/hw/routers/ps368/index.html

The supported configuration for the HA based on the 7600 Series switch is dependent on the desired capacity, interface type to be deployed and whether IPSec support is required.

Before you install the Cisco HA, keep the following considerations in mind:

The SAMI requires either a Supervisor Engine 32, or a Supervisor Engine-720 (WS-SUP720-3BXL), with MSFC-3 (WS-SUP720)/PFC-3 (WS-F6K-PFC3BXL). For details, see the "Upgrading to a New Software Release" section in the Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers. SRB1 or higher is required for Sup32 and Sup720, and SRC is required for RSP720.

A Cisco SAMI module is required to run HA functionality. Each SAMI module supports 1 HA logical instance running on 6 processors.

For IPSec support, an IPSec VPN accelerator for the Catalyst platform (VPNSPA) is required per 7600 chassis.

Cisco MW HA Release 12.4(22)YD is supported on the following platforms:

- Cisco 7600 Internet Router platform—Please refer to the following URL for installation and configuration information:

  http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/pref.html

Software Compatibility

Cisco IOS Release 12.4(22)YD is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(22)YD supports the same features that are in Cisco IOS Release 12.4, with the addition of the Cisco Mobile Wireless HA feature.

Determining the Software Version

To determine the version of Cisco IOS software running on your router, log in to the router and enter the **show version** EXEC command:

```
Router#show version
Cisco IOS Software, SAMI Software (SAMI-H2IK9S-M), Version 12.4(22)YD, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 02-Feb-09 17:45 by prod_rel_team

ROM: System Bootstrap, Version 12.4(20080703:222712) [plin2-sami-bouncer 104], DEVELOPMENT
SOFTWARE

Router uptime is 18 hours, 34 minutes
System returned to ROM by reload at 19:04:03 UTC Tue Feb 10 2009
System restarted at 19:08:46 UTC Tue Feb 10 2009
System image file is "c7svcsami-h2ik9s-mz.124-22.YD.fc3"
Last reload reason: Reload command by admin
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco Systems SAMI (MPC8500) processor (revision 1.1) with 983040K/65536K bytes of memory.
Processor board ID SAD10210754
FS8548H CPU at 1250MHz, Rev 2.0, 512KB L2 Cache
1 Gigabit Ethernet interface
65536K bytes of processor board system flash (AMD S29GL256N)

Configuration register is 0x2102
```

Upgrading the SAMI Software

The SAMI comes preloaded with the operating system software. However, to take advantage of new features and bug fixes, you can upgrade your SAMI with a new version of the software when it becomes available.

The SAMI software (image name c7svcsamifeature-mz) is a bundle of images - comprised of images for the base card and daughter card components.

Each image in the bundle has its own version and release numbers. When an upgrade is initiated using the upgrade hw-module privileged EXEC command, the version and release numbers in the bundle are compared to the versions currently running. If the versions are different, that image is automatically upgraded.

Note The show module command displays the software version of the LCP image, not the version of the full SAMI bundle.

To upgrade the SAMI image, perform the following tasks:

	Command	Purpose
Step 1	`Sup> enable`	Enters privileged EXEC mode.
Step 2	`Sup# upgrade hw-module slot slot_num software file` *`url/file-name`*	Copies the bundled image from the specified URL to the compact flash.
Step 3	`Sup# hw-module module` *`slot_num reset`*	Resets the module by turning the power off and then on. SAMI resets using the new images.

	Command	Purpose
Step 4	`Sup# show upgrade software progress`	Displays status of the upgrades that are occurring.
Step 5	`Sup# show module` *`slot_num`*	Ensures that the SAMI card comes up properly after the reset. The status of the SAMI should be "OK".

Here is an example of the **show module** command:

```
sup#show module 2
Mod Ports Card Type Model Serial No.
--- ----- -------------------------------------- ------------------ -----------
2 1 SAMI Module (h2ik9s) WS-SVC-SAMI-BB-K9 SAD121202UK

Mod MAC addresses Hw Fw Sw Status
--- ---------------------------------- ------------ ------------ -------
2 001f.6c89.0dca to 001f.6c89.0dd1 2.2 8.7(0.22)FW1 12.4(2009020 Ok

Mod Sub-Module Model Serial Hw Status
---- --------------------------- ------------------ ----------- ------- -------
2 SAMI Daughterboard 1 SAMI-DC-BB SAD121204DZ 1.1 Ok
2 SAMI Daughterboard 2 SAMI-DC-BB SAD121204CL 1.1 Ok

Mod Online Diag Status
---- -------------------
2 Pass
```

For example, to perform an image upgrade on a SAMI in slot 2 of the Cisco 7600 chassis, enter the following commands:

```
Sup>
Sup> enable
Sup# upgrade hw-module slot 2 software file
tftp://10.1.1.1/c7svcsami-h2ik9s
Loading c7svcsami-h2ik9s from <TFTP SERVER IPADDRESS> (via Vlan10):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 34940891 bytes]
Sup# hw-module module 2 reset
Proceed with reload of module?[confirm]
% reset issued for module 2
Sup#
Apr 18 17:53:16.149 EDT: SP: The PC in slot 2 is shutting down. Please wait ...
Apr 18 17:53:33.713 EDT: SP: PC shutdown completed for module 2
000151: Apr 18 17:53:33.713 EDT: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off
(Reset)
000152: Apr 18 17:57:52.033 EDT: %MLS_RATE-4-DISABLING: The Layer2 Rate Limiters have been
disabled.
000153: Apr 18 17:57:51.513 EDT: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimal
Diagnostics...
000154: Apr 18 17:57:51.537 EDT: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
000155: Apr 18 17:57:52.073 EDT: %OIR-SP-6-INSCARD: SAMI inserted in slot 2, interfaces
are now online
000156: Apr 18 17:57:59.589 EDT: %SVCLC-5-FWTRUNK: Firewalled VLANs configured on trunks
Sup#
```

SAMI Configuration Instructions

The following instructions outline the steps needed to install a new SAMI and configure it so that an application image is booting on the PPCs. These instructions assume that this is a brand new SAMI, not a board being transferred from another chassis.

Upgrade Supervisor Image

You might need a new SUP image in order to recognize the SAMI. The SAMI requires either a Supervisor Engine 32, or a Supervisor Engine-720 (WS-SUP720-3BXL), with MSFC-3 (WS-SUP720)/PFC-3 (WS-F6K-PFC3BXL). For details, see the "Upgrading to a New Software Release" section in the Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers. SRB1 or higher is required for Sup32 and Sup720, and SRC is required for RSP720.

Insert the Board into the Chassis

After reloading the SUP, insert the SAMI into the chassis. Make sure to select a slot that has an empty slot above it so the cables can be easily connected.

Set up and connect a console port for the Itasca/LCP console. Also, set up and connect console ports to the PPC1 console. Even if only one will be used initially, there is a front panel port for each daughter card that will be enabled shortly. It will allow multiplexed access to all 3 processors.

Boot SAMI from the SUP

Perform the following tasks to boot the SAMI card from the SUP:

Step 1 Copy the latest LCP image to your TFTP server.

Step 2 Copy the image to the SUP.

Step 3 Add the following to the SUP configuration:

```
boot device module {slot} disk0:sb-csg2-image.bin
```

Step 4 Boot the board (LCP Console):

```
boot eobc:
```

Step 5 After the SAMI card boots, log in using "admin" as both the username and password.

Upgrade the LCP ROMMON

The following steps illustrate how to upgrade the LCP ROMMON:

Step 1 Copy the latest stable LCP ROMMON image.

Step 2 Copy the latest LCP ROMMON image to the Itasca compact flash.

Step 3 Upgrade the ROMMON:

```
reprogram bootflash fur-image image:rommon-image
```

Step 4 Reload the blade (LCP Console):

```
reload
boot eobc: (from the rommon prompt)
```

Boot SAMI from Itasca CF

The following steps illustrate how to boot the SAMI from the Itasca compact flash:

Step 1 Copy the latest LCP image to the Itasca compact flash. Example (from LCP console).

Step 2 Add the boot command to the Itasca configuration:

```
boot system image:sb-csg2-mzg.bin
```

Note Remove any existing boot system commands first.

Step 3 Change the config register to auto boot the Itasca.

```
config-register 1
```

Step 4 Reload the board.

Reprogram ROMMON on PPCs

To reprogram the ROMMON on the PPCs, perform the following tasks:

Step 1 Copy the latest LCP ROMMON image.

Step 2 Copy the image to the Itasca.

Step 3 Restart a PPC. Example (from LCP console):

```
testdc upgrade-rommon BOUNCER_RM.bin
```

Step 4 Set the ppc rommon to autoboot. Example (from the PPC console):

```
confreg 0x2102
```

Load and Run PPC Image

Perform the following tasks to load and run the PPC image:

Step 1 Copy the latest stable ppc application image.

Step 2 Copy the image to the Itasca. Example:

```
copy tftp://64.102.16.25/{username}/svcsami-h2ik9s.sami
image:svcsami-h2ik9s.sami_060626
```

Step 3 Restart a PPC. Example (from LCP console):

```
testdc restart svcsami-h2ik9s.sami_060626 proc 1
```

Required Base Configuration

A typical HA configuration requires that you define interfaces in three directions: PDSN/FA, home network, and AAA server. If HA redundancy is required, then you must configure another interface for HSRP binding updates between HAs. If you are running the HA on the SAMI, the HA will see the access to one GE port that will connect to Catalyst 7600 backplane. That port can be configured as a trunk port with subinterfaces provided for each necessary network access.

VLANs can be defined corresponding to each interface: PDSN/FA, home network, AAA. In the case of multiple HA instances in the same 7600 chassis, the same VLAN can be used for all of them.

The section Basic IOS Configuration on Supervisor for SAMI Module illustrates the required base configuration for the Cisco Mobile Wireless Home Agent.

Basic IOS Configuration on Supervisor for SAMI Module

To configure the Supervisor engine to recognize the SAMI modules, and to establish physical connections to the backplane, use the following commands:

	Command	Purpose
Step 1	`sup-7602(config)#vlan 3`	Add an Ethernet VLAN. Enters vlan configuration submode.
Step 2	`sup-7602(config-vlan)#exit`	Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode.
Step 3	`sup-7602(config)#interface vlan 3`	
Step 4	`sup-7602(config-if)# ip address 3.3.3.25 255.255.255.0`	
Step 5	`sup-7602(config)#vlan 30`	
Step 6	`sup-7602(config-vlan)#exit`	
Step 7	`sup-7602(config)#interface vlan 30`	
Step 8	`sup-7602(config-if)# ip address 30.0.0.25 255.0.0.0`	
Step 9	`sup-7602#svclc vlan-group 1 3`	

	Command	Purpose
Step 10	`sup-7602#svclc vlan-group 2 30`	
Step 11	`sup-7602#svclc module 8 vlan-group 1,2`	

For information on SAMI configuration details, please go to the following URL:

http://www.cisco.com/en/US/docs/wireless/service_application_module/sami/user/guide/samiv1.html

Note SAMI modules synchronize their timing functions from the Supervisor engine's clock timers. Do not configure the timers on each individual SAMI.

MIBs

Home Agent Release 5.0 introduces two new MIBs:

- CISCO-SLB-DFP-MIB
- CISCO-RADIUS-MIB

And the following MIBs are updated:

- CISCO-MOBILE-IP-MIB
- RADIUS-CLIENT-AUTHENTICATION-MIB

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 2.

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be decided
OLD-CISCO-DECNET-MIB	To be decided
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be decided
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be decided
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be decided

Cisco IOS Feature Sets

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.4(22)YD supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(22)YD includes the Cisco Mobile Wireless Home Agent feature. The HA 5.0 feature set is optimized for the Cisco SAMI blade on the 7600 Internet router.

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 are likely to require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, 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.

Cisco Mobile Wireless Home Agent Software Features in Release 12.4(22)YD

The Cisco IOS Release 12.4(22)YD supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(22)YD includes the HA feature. The Cisco HA feature is optimized for the Cisco SAMI blade on the 7600 Internet router, and includes the following features:

This section lists features that were introduced or modified in Home Agent Release 5.0 for Cisco IOS Release 12.4(22)YD:

- Single IP Infrastructure
- Home Agent Session Redundancy Infrastructure
- Automatic Intra-Chassis Configuration Synchronisation
- Bounded Limit For Maximum Bindings
- Congestion Control Feature
- Foreign Agent Classification
- MAC Address as Show/Clear Binding Key
- Data Path Idle Timer
- Support for RFC 4917
- Address Assignment Feature
- Accounting Interim Sync
- RADIUS Accounting Support in Single IP Home Agent infrastructure
- Global Per Domain Accounting
- Support for Acct-Terminate-Cause
- Authentication Configuration Extension

This section lists features that were introduced or modified before Cisco IOS Release 12.4(22)YD:

- Support for Service and Application Module for IP (SAMI)

- Up to 9 SAMI cards can be supported in a single Cisco 7600 Series Router chassis.
- Enhancements to Hot-lining
- Enhancements to Home Agent Quality of Service
- Framed-Pool Standard
- WiMAX AAA Attributes
- MS Traffic Redirection in Upstream Path
- Per Foreign-Agent Access-Type Support
- Priority-Metric for Local Pool
- Mobile IPv4 Host Configuration Extensions RFC4332
- Support for Mobile Equipment Identifier (MEID)
- Home Agent Accounting Enhancements
- Home Agent Accounting in a Redundant Setup
- Packet count and Byte count in Accounting Records
- Additional Attributes in the Accounting Records
- Additional Accounting Methods—Interim Accounting is Supported.
- VRF Mapping on the RADIUS Server
- Conditional Debugging Enhancement
- Home Agent Redundancy Enhancements
- Redundancy with Radius Downloaded Pool Names
- CLI for IP-LOCAL-POOL-MIB
- Mobile-User ACLs in Packet Filtering
- IP Reachability
- DNS Server Address Assignment
- Mobile IP MIB Enhancements in Network Management, MIBs, and SNMP on the Home Agent
- Mobile IPv4 Registration Revocation
- HA Server Load Balancing
- Home Agent Accounting
- Skip HA-CHAP with MN-FA Challenge Extension (MFCE)
- VRF Support on HA
- Radius Disconnect
- Conditional Debugging
- Home Address Assignment
- Home Agent Redundancy
- Virtual Networks
- Mobile IP IPSec
- Support for ACLs on Tunnel Interface
- Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY
- 3 DES Encryption

- User Profiles
- Mobility Binding Association
- User Authentication and Authorization
- HA Binding Update
- Per User Packet Filtering
- Security

Feature Support

In addition to supporting Cisco IOS networking features, a Cisco 7600 series router configured as a Home Agent, supports the following Home Agent-specific features:

- Support for both intra-chassis and inter-chassis HA redundancy
- Support for static IP addresses assignment
  - Public IP addresses
  - Private IP addresses
- Support for dynamic IP addresses assignment
  - Public IP addresses
  - Private IP addresses
- Multiple flows for different Network Access Identifiers (NAIs) using static or dynamic addresses
- Multiple flows for the same NAI using different static addresses
- Foreign Agent Challenge extensions in RFC 3012 - bis 03
  - Mobile IP Agent Advertisement Challenge Extension
  - MN-FA Challenge Extension
  - Generalized Mobile IP Authentication Extension, which specifies the format for the MN-AAA Authentication Extension
- Mobile IP Extensions specified in RFC 2002
  - MN-HA Authentication Extension
  - FA-HA Authentication Extension
- Reverse Tunneling, RFC 2344
- Mobile NAI Extension, RFC 2794

- Multiple tunneling modes between FA and HA
  - IP-in-IP Encapsulation, RFC 2003
  - Generic Route Encapsulation, RFC 2784
  - MIP-UDP tunneling
- Binding Update message for managing stale bindings
- Home Agent redundancy support
- Mobile IP Extensions specified in RFC 3220
  - Authentication requiring the use of SPI. section 3.2
- Support for Packet Filtering
  - Input access lists
  - Output access lists
- Support for proxy and gratuitous ARP
- Mobile IP registration replay protection using time stamps. Nonce-based replay protection is not supported.

All other software features in Cisco IOS Release 12.4 are described in the documentation for Cisco IOS Release 12.4, which can be found at:
http://www.cisco.com/en/US/products/ps6350/tsd_products_support_series_home.html

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

Caveats for Cisco IOS Releases 12.4 can be found on CCO at
http://www.cisco.com/en/US/products/ps6350/prod_release_notes_list.html

The Open Caveats section lists open caveats that apply to the current release and might also apply to previous releases.

The Resolved Caveats section lists caveats resolved in a particular release, which may have been open in previous releases.

Note If you have an account with CCO, you can use the Bug Toolkit to find caveats of any severity for any release. You can reach the Bug Toolkit at
http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

Open Caveats

There are no unresolved caveats in Cisco IOS Release 12.4(22)YD.

Resolved Caveats

The following caveats are resolved in Cisco Home Agent Release 12.4(22)YD:

- CSCsu11522

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

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

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml.

- CSCsu70214

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

- CSCsv04836

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

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

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

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

- CSCsv38166

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

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

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

Cisco has released free software updates that address this vulnerability.

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

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

- CSCsv75948

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at the following link:

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

Related Documentation

Except for feature modules, documentation is available as printed manuals or electronic documents. Feature modules are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 15
- Platform-Specific Documents, page 15

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.4T:

- *Cisco Mobile Wireless Home Agent Feature for Cisco IOS Release 12.4(22)YD* at the following url:

  http://www.cisco.com/en/US/products/ps6706/products_feature_guides_list.html

Platform-Specific Documents

Documentation specific to the Cisco 7600 Router is located at the following location:

- On Cisco.com at:
  http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, 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

---