Release Notes for Cisco IAD2801 Series Integrated Access Devices with Cisco IOS Release 12.4(20)YA

First Released: January 16, 2008
Last Revised: April 7, 2009
Cisco IOS Release 12.4(20)YA3
OL-18978-02 Second Release

These release notes for the Cisco IAD2801 Series Integrated Access Devices describe the product-related enhancements provided in the Cisco IOS Release 12.4(20)YA. These release notes are updated as needed.

For a list of the applicable software caveats, see the "Caveats" section on page 5. *See also Caveats for Cisco IOS Release 12.4(20)T*, which is updated for every maintenance release.

Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* and *About Cisco IOS Release Notes*.

Contents

These release notes describe the following topics:

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

Introduction

The following Cisco IAD2801 models are supported:

- IAD2801-2BRI-A/K9- Fixed configuration router, with integrated PVDM2-8, HWIC-1ADSL, and 1 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot
- IAD2801-4BRI-A/K9- Fixed configuration router, with integrated PVDM2-16, HWIC-1ADSL, and 2 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot.
- IAD2801-4BRI-S/K9- Fixed configuration router, with integrated PVDM2-16, HWIC-4SHDSL, and 2 VIC2-2BRI-NT/TE-P, 2 Fast Ethernet connections, and 1 factory configurable HWIC slot

The following cards are supported in the factory configurable HWIC slot on all models:

- HWIC-4ESW
- VIC-4FXS
- HWIC-AP-AG-E or HWIC-AP-G-E

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.4(20)YA, see the "New and Changed Information" section on page 3.

System Requirements

This section describes the system requirements for the Cisco IOS Release 12.4(20)YA releases and includes the following sections:

Memory Requirements

Table 1 lists the memory requirements for the Cisco IOS feature sets on the Cisco IAD2801 in Cisco IOS Release 12.4(20)YA. The Cisco IAD2801 uses a 32-MB Flash memory card.

Table 1 Cisco Release 12.4(20)YA Memory Requirements for the Cisco IAD2801 Series IAD

Platform	Feature Set	Software Image	Flash Memory (MB)	DRAM Memory (MB)	Runs From
Cisco IAD2801	Cisco IAD2801 IOS Advanced IP Services	ciad2801-advipservices k9-mz	64	256	RAM
Cisco IAD2801	Cisco IAD2801 IOS SP Services	ciad2801-spservicesk9-mz	64	256	RAM

Hardware Supported

Cisco IOS Release 12.4(20)YA supports the Cisco IAD2801 series IADs.

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 3.

For information about supported hardware for this platform and release, see the *Hardware/Software Compatibility Matrix* at:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Determining the Software Release

To determine the version of Cisco IOS software currently running on your Cisco IAD2801 series router, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

Feature Set Tables

For information about Feature Set Tables, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

New and Changed Information

The following sections list the new hardware products and software features supported by the Cisco IAD2801 in Cisco IOS Release 12.4(20)YA:

New Hardware Features in Cisco IOS Release 12.4(20)YA3

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(20)YA3

There are no new software features in this release.

New Hardware Features in Cisco IOS Release 12.4(20)YA2

There are no new hardware features in this release.

New Software Features in Cisco IOS Release 12.4(20)YA2

There are no new software features in this release.

Limitations and Restrictions

The following limitations and restrictions apply to the Cisco IAD 2801 series

Fixed Configuration Platforms Supporting Specific Cards

The Cisco IAD2801 series are fixed configuration platforms with each slot supporting specific cards. Supported cards in each model are shown below:

Table 2 Supported Cards in Cisco IAD2801 Series

Platform	Slot 0	Slot 1	Slot 2	Slot 3
IAD2801-2BRI-A/K9	VIC2-2BRI-NT/TE-P	HWIC-1ADSL	Not Available	LTD Option[1]
IAD2801-4BRI-A/K9	VIC2-2BRI-NT/TE-P	HWIC-1ADSL	VIC2-2BRI-NT/TE-P	LTD Option[1]
IAD2801-4BRI-S/K9	VIC2-2BRI-NT/TE-P	HWIC-4SHDSL	VIC2-2BRI-NT/TE-P	LTD Option[1]

1. LTD OPTION (Factory installable or Field Upgradable)

- HWIC-AP-AG-E and HWIC-AP-G-E
- HWIC-4ESW
- VIC-4FXS/DID

Unsupported Card Message

If any unsupported card is detected during the bootup, the following message appears:

"Card is not supported in slot 2. Please remove it."

This message appears for each unsupported card detected.

If any cards are not supported and **smart-init** is enabled, another message appears during bootup:

```
Smart Init is enabled
smart init is sizing iomem
 ID             MEMORY_REQ         TYPE
                 0X003AA110 public buffer pools
                 0X00211000 public particle pools
                 0X00020000 Crypto module pools
                 0X00120000 VPM buffer pools
0X05B3           0X000034A0 Card in slot 0
0X04C8           0X00077D00 Card in slot 1
0X05B3           0X00000000 UNKNOWN Card in slot 2
0X003A           0X00000000 Card in slot 3
                 0X000021B8 Onboard USB
```

Caveats

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

This section contains the following caveat information:

Open Caveats - Cisco IOS Release 12.4(20)YA3

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(20)YA3

CSCsu84868 c3845: Error mesg %SYS-2-BADSHARE: Bad refcount in datagram_done.

Symptom Cisco 3845 experiences trackback error:

Aug 14 12:34:55.960: %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=7006C010, count=0, -Traceback= 0x61816650 0x60641BD0 0x60C27A80 Aug 17 16:51:45.739: %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=705985A4, count=0, -Traceback= 0x61816650 0x60641BD0 0x60C27A80

Conditions The error message occurs on a router running the c3845-adventerprisek9_ivs_li-mz.124-15.T5 image.

Workaround None.

CSCsy22826 VG224 sending incorrect ssType in 1+ node CUCM cluster.

Symptom VG224 endpoint does not connect to callback destination, once the callback destination is idle.

Conditions Multi node cluster and VG224 endpoint is registered with node other then the first node in the cluster.

Workaround Have VG224 endpoints registered with first node.

Further Problem Description: The activation of the callback is successful. What fails is when the callback destination becomes idle again and the VG224 endpoint gets notified (ring). After the VG224 endpoint goes offhook, the system should automatically connect to the Callback destination.This does not happen and VG224 endpoint gets silence.

Open Caveats - Cisco IOS Release 12.4(20)YA2

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(20)YA2

CSCsr16693

A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

CSCsu21828

A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

CSCsv38166

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

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

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

Cisco has released free software updates that address this vulnerability.

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

This advisory is posted at the following link:

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

CSCsu11522

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

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

This advisory is posted at the following link:

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

CSCsk64158

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

Conditions Cisco has released free software updates that address this vulnerability.

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

CSCsk41593 PAK_SUBBLOCK error found when ping with >1500-byte over cellular inter.

Symptom The following error occurs when a ping packet is sent or received:
PAK_SUBBLOCK_ALREADY: 2 -Process= "IP Input"

Conditions Occurs when large ping packets (greater than 1500 bytes) are sent to back-to-back cellular interfaces with GRE tunneling enabled.

Workaround Disable the **<CmdBold>ip virtual-reassembly<noCmdBold>** command on the cellular interface.

CSCso30142 Traceback due to channel-group configuration.

Symptom Traceback is generated during boot up.

Conditions This is caused when the channel-group serial interface is configured with ip-address or np-ip-address. This is specific to T1/E1 HWIC.

Workaround None.

CSCso39750 router crashes at socket_inherit_fd after no ccm sccp.

CSCso39964 QoS:router hangs while removing class-map.

Symptom The router hangs when attempts are made to modify pure ACL configuration while traffic is still flowing.

Conditions Occurs on routers running Cisco IOS Release 12.4(15)T4. The router returns back to normal if the traffic is stopped.

Workaround There is no workaround.

CSCso41513 helper-address triggers ARP for non directly connected server.

Symptom When using the **<CmdBold>ip helper-address<noCmdBold>** command to forward directed broadcast, an incomplete ARP entry will be created for the helper-address configured even if it is not a directly connected subnet. This may break BOOTP forwarding to the DHCP server.

Conditions The symptoms are observed in Cisco IOS Release 12.4(19) only. Cisco IOS Release 12.4(18) does not have this issue.

Workaround Configure proxy-arp on the next hop device on the path to the DHCP server.

Alternate Workaround: Configure static ARP on the router for the helper-address pointing towards the next hop.

CSCso52548 parser breakage in crypto isakmp key <> CLI.

Symptom crypto isakmp key cli parser mode breakage.

Conditions crypto isakmp key <> cli.

Workaround None.

Further information: Not service impacting. Only that, crypto isakmp key <0/6> ? option gives "% Ambiguous command" instead of WORD for (UNENCRYPTED/ENCRYPTED) password.

CSCso61743 Router crashes@stcapp_free_supported_codec_list when stop/start stcapp.

Symptom Router crashes when stcapp is disabled, stcapp ccm-group is removed from configuration, and then stcapp is re-enabled.

Conditions Occurs on Cisco 2691 and Cisco 3745 routers running Cisco IOS Release 12.4(15)T05. Can also occur on other platforms running this Cisco IOS release. Can also occur if stcapp is disabled and the user attempts to enable stcapp but stcapp fails to start for any reason.

Workaround None.

CSCsq20970 ATM option missing, while configuring T1 controller for mode atm.

Symptom On the 2432 platform UUT, the 'atm' option is missing in the 'mode' CLI when the T1 controller is being configured for ATM.

Conditions The symptom is observed on the 2432 platform with a T1 controller.

Workaround There is no workaround.

CSCsq91960 failed to delete vrf when it is 32 characters long.

Symptom VRF may not get deleted if the VRF NAME size is 32 characters on a dual RP HA/SSO router.

Conditions This symptom occurs when adding a VRF with 32 characters on a DUAL RP HA router. (In some releases a VRF name with more than 32 characters will get truncated to 32.) The following may occur:

- There may be a DATA CORRUPTION ERRMSG.
- While deleting this 32 character length VRF, VRF will fail to get deleted completely with an ERRMSG on active.

Workaround There is no workaround.

CSCsq97697 No dialtone is heard when an outgoing call is made right after call disc.

Symptom Sometimes dialtone is not heard when user disconnects the existing call and immediately makes another outgoing call via hookflash.

Conditions Is seen when hookflash is used to disconnect the existing call and make an outgoing call.

Workaround Do not use the hookflash button. Go onhook to disconnect the call, wait for a few seconds then go offhook to make a new outgoing call.

CSCsr06625 telephony-service command throws % Invalid input detected.

CSCsr27960 Traceback observed after configuring credential under sip-ua.

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

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

Workaround There is no workaround.

CSCsr68545 Error %DATACORRUPTION-1-DATAINCONSISTENCY when running ipsla with rtt.

Symptom Error message occurs:
000302: Jul 24 13:00:13.575 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copyerror -Traceback= 0x410FD1A4 0x41119DB0 0x41138324 0x41DE5714

Conditions IP SLA configured with RTT.

Workaround There is no workaround.

CSCsr74835 incorrect uses of sprintf() in tcp/telnet.c.

Symptom Certain sprintf() calls in tcp/telnet.c are incorrect.

Conditions They have the potential to overflow the destination buffers.

Workaround snprintf() should be used with a bounding length of the size of the destination buffer.

CSCsr78883 Router console displays messages "Data corruption Data Inconsistency.

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

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

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

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

CSCsr92741 TCP packets with zero fields misbehavior.

Symptom When a TCP packet with all fields set to "zero" (at a tcp level) is sent to a remote router (whether using ipv4 and IPv6). The destination router (to which the destination IP belongs), will send a ACK/RST flag set TCP packet back to the source.

Workaround CoPP, FPM and other mechanisms can be used to mitigate and protect against these packets.

CSCsu18029 IAD2801 routers not booting up

CSCsu24050 Multiple PRC_NON_COMPLIANCE tracebacks found on configuring stcapp FAC.

CSCsu58305 c880 build breaks due to stricter compiler flags in the throttle branch.

CSCsu64215 ip tcp adjust-mss command results in packet loss for non-TCP traffic.

Symptom Router may incorrectly drop non TCP traffic. TFTP and EIGRP traffic can be impacted as seen in CSCsv89579.

Conditions Occurs when the **<CmdBold>ip tcp adjust-mss<NoCmdBold>** command is configured on the device.

Workaround Disable **<CmdBold>ip tcp adjust-mss<NoCmdBold>** on all interfaces. Note that this may cause higher CPU due to fragmentation and reassembly in certain tunnel environments where the command is intended to be used.

CSCsv13562 Router crashes due to double free of ccb->call_info.origRedirectNumber.

Symptom The router crashes due to double free scenarios. While handling 302 response, "ccb->call_info.origRedirectNumber" attempts a double free due to signaling forking.

Conditions Running Call Manager Express.

Workaround There is no workaround.

CSCsv54651 Crafted VTP packet could cause a crash.

Cisco's VTP protocol implementation in some versions of Cisco IOS and CatOS may be vulnerable to a DoS attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash (and reload/hang). The crafted packet must be received on a switch interface configured to operate as a trunk port.

Workaround None.

This response is posted at http://www.cisco.com/warp/public/707/cisco-sr-20081105-vtp.shtml

CSCsv84605 When phone is onhook, media shouldn't be handled.

Symptom Reporting port hang. The symptom is that when the port is blocked, the underlying low layer (VPM, VTSP) is already in clean IDLE state, but STCAPP keeps itself in the REM_ONHOOK_PEND -> CONNECTING -> ACTIVE_PENDING -> ONHOOK_PEND -> REM_ONHOOK_PEND loop.

Conditions When STCAPP is used for analog phones through CCM control. CCM is 6.1.1. STCAPP version is 12.4(20)YA1. The fix will go into 12.4(22)T.

Workaround None.

Resolved Caveats - Cisco IOS Release 12.4(20)YA1

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.

CSCsw47076

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.

CSCsv48603

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.

CSCsx07114

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.

CSCsu50252

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.

CSCsy54122

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.

CSCsy15227

Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at the following link:

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

CSCsz38104

The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml.

CSCsq58779

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

Cisco has released free software updates that address this vulnerability.

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

CSCsr18691

Cisco IOS devices that are configured with Cisco IOS Zone-Based Policy Firewall Session Initiation Protocol (SIP) inspection are vulnerable to denial of service (DoS) attacks when processing a specific SIP transit packet. Exploitation of the vulnerability could result in a reload of the affected device.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available within 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-ios-fw.shtml

CSCsy07555

Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

Cisco has released free software updates that address this vulnerability.

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

CSCee72997

Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml

CSCsu24505

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

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

CSCsx25880

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

CSCsq24002

Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml.

CSCsq31776

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.

CSCsx70889

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

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

CSCsh97579

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

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

Additional References

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

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.4(20)YA.

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

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 2800 series routers are at:

http://www.cisco.com/en/US/products/ps7214/tsd_products_support_series_home.html

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.

Notices

See the "Notices" section in *About Cisco IOS Release Notes* located at: http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

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

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