Release Notes for Cisco 1800 Series Routers with Cisco IOS Release 12.4(20)YA

First Released: August 1, 2008
Last Revised: April 7, 2009
Cisco IOS Release 12.4(20)YA3
OL-17462-04 Fourth Release

These release notes describe new features and significant software components for the Cisco 1800 series routers that support Cisco IOS Release 12.4(20)YA. These release notes are updated as needed. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* and *About Cisco IOS Release Notes*

For a list of the software caveats that apply to the Release 12.4(20)YA releases, "Caveats" section on page 7, and see the online *Caveats for Cisco IOS Release 12.4(20)T*

Contents

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

System Requirements

following sections:

Memory Requirements

Table 1 Memory Requirements for the Cisco 1800 Series Routers

Platform	Image Name	Image	Flash (MB)	RAM (MB)
Cisco 1803 Cisco 1805	Cisco 1800 Series IOS Advanced Enterprise Services	adventerprisek9-mz	32	128
	Cisco 1800 Series IOS Advanced IP Services	advipservicesk9-mz	32	128
	Cisco 1800 Series IOS IP Broadband	broadband-mz	32	128
Cisco 1811 Cisco 1812	Cisco 1811 Series IOS Advanced Enterprise Services	adventerprisek9-mz	32	128
	Cisco 1811 Series IOS Advanced IP Services			
Cisco 1811	Cisco 1811 Series IOS Advanced IP Services	advipservicesk9-mz	32	128

(continued)

Cisco 1841	Cisco 1841 IOS Advanced Enterprise Services	adventerprisek9-mz	64	192
	Cisco 1841 IOS AISK9-AESK9 Feature Set Factory Upgrade For Bundles	adventerprisek9-mz	64	192
	Cisco 1841 IOS ASK9-AESK9 Feature Set Factory Upgrade For Bundles		64	192
	Cisco 1841 IOS BB-AESK9 Feature Set Factory Upgrade For Bundles		64	192
	Cisco 1841 IOS Advanced IP Services	advipservicesk9-mz	64	128
	Cisco 1841 IOS ASK9-AISK9 Feature Set Factory Upgrade For Bundles		64	128
	Cisco 1841 IOS BB-AISK9 Feature Set Factory Upgrade For Bundles		64	192
	Cisco 1841 IOS AISK9-AISK9 Feature Set Factory Upgrade For Bundles		64	192
Cisco 1841	Cisco 1841 IOS Advanced Security	advsecurityk9-mz	64	192
	Cisco 1841 IOS BB-ASK9 Feature Set Factory Upgrade For Bundles		64	192
	Cisco 1841 IOS ASK9-ASK9 Feature Set Factory Upgrade For Bundles		64	192
	Cisco 1841 IOS Broadband	broadband-mz	32	128
	Cisco 1841 IOS BB-BB Feature Set Factory Upgrade For Bundles		32	128
	Cisco 1841 IOS Enterprise Base without Crypto	entbase-mz	64	128
	Cisco 1841 IOS Enterprise Base	entbasek9-mz	64	128
	Cisco 1841 IOS Enterprise Services without Crypto	entservices-mz	64	192
	Cisco 1841 IOS Enterprise Services	entservicesk9-mz	64	192
	Cisco 1841 IOS IP Base without Crypto	ipbase-mz	32	128
	Cisco 1841 IOS IP Base	ipbasek9-mz	32	128
	Cisco 1841 IOS SP Services	spservicesk9-mz	64	128
	Cisco 1841 IOS BB-SPSK9 Feature Set Factory Upgrade for Bundles	spservicesk9-mz	64	128
	Cisco 1841 IOS SPSK9-SPSK9 Feature Set Factory Upgrade for Bundles		64	128

Platform	Image Name	Image	Flash (MB)	RAM (MB)

Hardware Supported

-
-

. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1800 series routers, which are at:

http://www.cisco.com/en/US/products/ps5853/tsd_products_support_series_home.html

Determining the Software Version

Upgrading to a New Software Release

Feature Set Tables

New and Changed Information

-
-
-
-
-
-
-
-
-

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

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

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

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

New Hardware Features in Cisco IOS Release 12.4(20)YA1

New Software Features in Cisco IOS Release 12.4(20)YA1

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

-

NME-IPS-K9

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

Cisco Unified Communications including the following features for FXS ports on Cisco VG224 Analog Phone Gateways and Cisco integrated services routers:

Call Hold/Resume for Shared Lines for SCCP Analog Ports, page 6

Flexible Feature Access Codes, page 6

SIP Supplementary Features for Analog Ports on Cisco VG224/Cisco ISRs with Cisco Unified Communications Manager, page 6

Call Hold/Resume for Shared Lines for SCCP Analog Ports

Flexible Feature Access Codes

SIP Supplementary Features for Analog Ports on Cisco VG224/Cisco ISRs with Cisco Unified Communications Manager

-
- 3 Way Calling
- Call Transfer
- Call Waiting.

New Features in Release 12.4T

For information regarding the features supported in Cisco IOS Release 12.4T, see the links at:

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

Caveats

Open Caveats - Cisco IOS Release 12.4(20)YA3

Resolved Caveats - Cisco IOS Release 12.4(20)YA3

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

Symptom

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

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

Further Problem Description

CSCsr16693

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.

CSCsv38166

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.

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.

CSCsk64158

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

PAK_SUBBLOCK_ALREADY: 2 -Process= "IP Input"

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

Disable the **<CmdBold>ip virtual-reassembly<noCmdBold>**

CSCso39750 router crashes at socket_inherit_fd after no ccm sccp.

CSCso39964 QoS:router hangs while removing class-map.

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

Alternate Workaround:

CSCso52548 parser breakage in crypto isakmp key <> CLI.

crypto isakmp key <> cli.

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.

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

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

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

CSCsr06625 telephony-service command throws % Invalid input detected.

CSCsr27960 Traceback observed after configuring credential under sip-ua.

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

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

IP SLA configured with RTT.

There is no workaround.

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

CSCsr78883 Router console displays messages "Data corruption Data Inconsistency.

mls qos cos pass-through dscp

mls qos cos pass-through dscp

mls qos cos override | cos-value

Further Problem Description
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.

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.

<CmdBold>ip tcp adjust-mss<NoCmdBold>

<CmdBold>ip tcp adjust-mss<NoCmdBold>

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

CSCsu70214

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

CSCsu50252

CSCsy54122

CSCsy15227

CSCsz38104

CSCsq58779

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

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

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

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

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

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.

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.

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.

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.

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.

The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

Note

Symptom

Conditions

Workaround

Symptom

Workaround

Symptom

Conditions

Workaround

Symptom

Workaround

Symptom

Conditions

Workaround

Open Caveats - Cisco IOS Release 12.4(20)YA

Resolved Caveats - Cisco IOS Release 12.4(20)YA

Additional References

-

-

Release-Specific Documents

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

Platform-Specific Documents

Cisco IOS Software Documentation Set

Documentation Modules

Notices

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