Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.0(30)SZ10

First Published: May 2009

Last Revised: September 2009

These release notes provide information about Cisco IOS Release 12.0(30)SZ10 for the Cisco 10000 series router. This release is a maintenance release and has no new features.

For a list of the software caveats that apply to Cisco IOS Release 12.0(30)SZ10, see the "Caveats for Cisco IOS Release 12.0(30)SZ10" section on page 4.

Cisco IOS Release 12.0(30)SZ10 is based on the following releases:

- Cisco IOS Release 12.0(30)S5
- Cisco IOS Release 12.0(30)SZ through Release 12.0(30)SZ9

To review the release notes for Cisco IOS Release 12.0S, go to:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/prod_release_notes_list.html

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.htm.

Contents

These release notes describe the following topics:

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

System Requirements

The following sections describe the system requirements for Cisco IOS Release 12.0(30)SZ10:

Supported Hardware

For Cisco IOS Release 12.0(30)SZ10, you must have the performance routing engine (PRE), Part Number ESR-PRE1, installed in the Cisco 10000 series chassis. To verify which PRE is installed in the router, use the **show version** command.

For information about line cards supported by Cisco 10000 series routers, see the "Supported Line Cards for the 10000 Series Routers" section in the *Cross-Platform Release Notes for Cisco IOS Release 12.0S, Part 1: System Requirements* at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/prod_release_note09186a00803c2dcb.html

Feature Support

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

Cisco IOS Release 12.0(30)SZ10 is based on Cisco IOS Release 12.0(30)S5 and subsequent Cisco IOS Release 12.0(30)SZ*x* maintenance releases. All features supported by Cisco IOS Release 12.0S up to and including Release 12.0(30)S5 are supported by Cisco IOS Release 12.0(30)SZ10.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [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 because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Upgrading to a New Software Release

The following sections provide information about upgrading your Cisco 10000 series router to a new software release:

Before You Upgrade the Cisco IOS Software

Before you upgrade (or downgrade) the Cisco IOS software running on the Cisco 10000 series router, save the running configuration file using the **copy** command. In route processor redundancy (RPR) mode, the router synchronizes only the startup configuration.

Information About Upgrading to a New Software Release

For specific information about upgrading your Cisco 10000 series router to a new software release, see the *Cisco 10000 Series Router Performance Routing Engine Installation* at:

http://www.cisco.com/en/US/products/hw/routers/ps133/prod_installation_guide09186a0080525aba.html

For general information about upgrading to a new software release, see the product bulletin *Cisco IOS Upgrade Ordering Instructions* at:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm#wp26467

For additional information about ordering Cisco IOS software, see the Products and Services Ordering website at:

http://www.cisco.com/en/US/ordering/index.shtml

New and Changed Features

Cisco IOS Release 12.0(30)SZ10 is a maintenance release and has no new hardware or software features.

For information about new features supported on the Cisco 10000 series router in other releases, see the appropriate release notes at:

http://www.cisco.com/en/US/products/hw/routers/ps133/prod_release_notes_list.html

For information about Cisco IOS Release 12.0(30)S, see the appropriate document at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/prod_release_notes_list.html

Important Notes

The following sections provide important information:

Inserting a New Line Card

Unlike other Cisco routers, if you insert a new or different line card into a Cisco 10000 series chassis slot that previously had a line card installed, the line card initially reports that it is administratively up.

Deferring Cisco IOS Software Images

Cisco IOS software images are subject to deferral. We recommend that you view the deferral notices at the following URL to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Caveats for Cisco IOS Release 12.0(30)SZ10

Caveats describe unexpected behavior in Cisco IOS software releases. This document includes caveats ranging from severity 1 to severity 3 only. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

Cisco IOS Release 12.0(30)SZ10 is based on Cisco IOS Release 12.0(30)S5 and Releases 12.0(30)SZ through 12.0(30)SZ9, and contains all of the open and resolved caveats in these releases. For information on the caveats in these releases, see the following release notes documents:

- For Cisco IOS Release 12.0(30)S5, see the *Cross-Platform Release Notes for Cisco IOS Release 12.0S, Part 3: Caveats for 12.0(30)S through 12.0(32)S6* at:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/prod_release_note09186a00803c2609.html

- For other Cisco IOS Release 12.0(30)SZ releases, see the release notes section titled "Cisco IOS Release 12.0SZ" at:

  http://www.cisco.com/en/US/products/hw/routers/ps133/prod_release_notes_list.html

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 12.2 > 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 request is not displayed, it might 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.)

The following sections describe open and resolved caveats for Cisco IOS Release 12.0(30)SZ10:

- Open Caveats in Cisco IOS Release 12.0(30)SZ10, page 4
- Resolved Caveats in Cisco IOS Release 12.0(30)SZ10, page 6

Open Caveats in Cisco IOS Release 12.0(30)SZ10

This section describes caveats that are open in Cisco IOS Release 12.0(30)SZ10.

CSCdy45049

During a lab stress test, line rate traffic does not always achieve line rate when the configuration scales to more than 3000 serial interfaces. This problem occurs only when thousands of serial interfaces with PPP or HDLC encapsulation are used on the port and line rate traffic is sent through all interfaces.

Workaround: No workaround is available.

CSCeh48414

During high availability (HA) testing of the Stateful Switchover (SSO) feature, traffic is not stable before or after the switchover occurs. This behavior occurs on a Cisco 10000 series router with 200 serial network interfaces, two channelized OC-12 interfaces, and one Ethernet interface. This symptom is observed on the 200 interfaces and only when the router is running Cisco IOS Release 12.0(25)SX10.

Workaround: No workaround is available.

CSCeh73497

After a route processor (RP) switchover, the following message is sometimes observed. This behavior occurs on the Cisco 10000 series router with redundant PRE1 cards and with RPR+ mode configured.

```
C10KEVENTMGR-1-IRONBUS_FAULT: Barium Error
```

The message results from an internal timing issue during the RP switchover. The affected line card recovers successfully and no performance impact is observed.

Workaround: No workaround is available.

CSCei93434

In a high availability (HA) environment with multilink point to point (MLPPP) interfaces configured, after a PRE cutover a small PXF buffer leak is observed. As shown in the following sample output, for buffer pool 3 the total number of buffers (67666) does not equal the number of available buffers (67139). This mismatch occurs when the router is running Cisco IOS Release 12.0(28)S4.

```
  pool   size    # buffer    available   allocate failures
 ---------------------------------------------------------
  0      9216    100            100        0
  1      4672    500            500        0
  2      1600    30000          30000      0
  3      640     67666          67139      0
  4      256     98165          98165      0
  5      64      131000         131000     0
```

Workaround: No workaround is available.

CSCej89322

Spurious memory access is observed at fib_notify_interface_state_change after the secondary switchover in the primary router. This symptom occurs on the router when running Cisco IOS Release 12.0(30)S4 and Release 12.0(28)S5.

Workaround: No workaround is available.

CSCsg51693

A random ping failure occurs between two CE routers and is randomly observed across different virtual private networks (VPNs) for more than 300 VPNs. The number of ping failures across the VPNs varies randomly. The number of VPNs is set to 500 and the number of VPN routes is set to 136. Ping operations between two PE routers are successful. The ping failure is not observed when the number of VPN routes is set to 0 and the number of VPNs is set to 999. This symptom occurs when the router is running Cisco IOS Release 12.0(30)SZ and Release 12.0(30)SZ2.

Workaround: No workaround is available.

Resolved Caveats in Cisco IOS Release 12.0(30)SZ10

This section describes caveats that were fixed in Cisco IOS Release 12.0(30)SZ10.

CSCeb69473

The device crashed with a segmentation violation (SegV) exception. This behavior occurred when the **connect** *target_ip* **[login|513] /terminal-type** *value* command was entered with a large input parameter to the *terminal-type* argument:

```
router>connect 192.168.0.1 login /terminal-type aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Trying 192.168.0.1...Open
login:

*** System received a SegV exception ***
signal= 0xb, code= 0x1100, context= 0x82f9e688
PC = 0x61616160, Vector = 0x1100, SP = 0x833ae5a8
```

AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. After the session is configured, the user is granted access to a requested service only if the information in the user profile allows it.

For a complete description of authorization commands, refer to the following links:

Configuring Authorization
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part05/schathor.htm

ACS 4.1 Command Authorization Sets
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/SPC.html#wpxref9538

ACS 4.1 Configuring a Shell Command Authorization Set for a User Group
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/GrpMgt.html#wp480029

Role-Based CLI Access—The Role-Based CLI Access feature allows the network administrator to define "views" which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices. The following link provides more information about the Role-Based CLI Access feature:

http://www.cisco.com/en/US/netsol/ns696/networking_solutions_white_paper09186a00801ee18d.shtml

Device Access Control—Due to the nature of this vulnerability, networking best practices such as access control lists (ACLs) and Control Plane Policing (CoPP) that restrict vulnerable device access to certain IP addresses or subnetworks may not be effective. Device access best practices provide some mitigation for these issues by allowing systemic control of authenticated and unauthenticated users. Device access best practices are described in the following document:

Infrastructure Protection on Cisco IOS Software-Based Platforms, Appendix B-Controlling Device Access
http://www.cisco.com/application/pdf/en/us/guest/products/ps1838/c1244/cdccont_0900aecd804ac831.pdf

Improving Security on Cisco Routers

http://www.cisco.com/warp/public/707/21.html

CSCsc94359

On a Cisco 10000 series router that functioned as a PE router, the BGP table and CEF forwarding table had mismatched labels for prefixes that were learned from a remote PE router. This problem has been fixed.

CSCsg00102

A device configured for SSL VPN stopped accepting new SSL VPN connections, due to a vulnerability in processing new TCP connections for SSL VPN services. When **debug ip tcp transactions** was enabled and the vulnerability triggered, debug messages with "connection queue limit reached" was observed. This problem has been fixed.

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.

CSCsi13344

Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

The Cisco Security Response is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml

See "Additional Information" section in the posted response for further details.

CSCsk64158

Several features within Cisco IOS software were affected by a crafted UDP packet vulnerability. If any of the affected features were enabled, a successful attack resulted 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 did not block the interface. This problem has been fixed.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available in the "Workarounds" section of the advisory at the following link:

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

CSCsm27071

A vulnerability while handling IP sockets caused devices to be susceptible to a denial of service (DoS) attack when any of the features of Cisco IOS Software were enabled. A sequence of specially crafted TCP/IP packets could have caused any of the following results:

- The configured feature stopped accepting new connections or sessions.
- The memory of the device was consumed.
- The device experienced prolonged high CPU utilization.
- The device was reloaded.

This problem has been fixed.

Cisco has released free software updates that address this vulnerability.Workarounds that mitigate this vulnerability are available in the "Workarounds"section at the following link:

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

CSCsm45113

The Cisco 10000 series router installed duplicate routes or an incorrect route netmask into the routing table. Additionaly a crash was observed for OSPF. This problem has been fixed.

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.

CSCsr74835

Potential overflow of the destination buffer was observed due to the unspecified bounding length of the size of the destination buffer. This problem has been fixed.

CSCsr92741

When a TCP packet with all fields set to zero (at TCP level) was sent to a remote router (using IPv4 and IPv6), the destination router (to which the destination IP belongs) sent an ACK/RST flag set ‘TCP packet’ back to the source. CoPP, FPM, and other mechanisms could be used to mitigate and protect against these packets. This problem has been fixed.

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.

CSCsv55537

After a Cisco 10000 series router was upgraded either from Cisco IOS Release 12.2(31)SB9a or 12.2(27)SB9b to Cisco IOS Release 12.2(31)SB9b , E1 flapped due to LOF/RMAI alarms. This problem has been fixed.

CSCsv55575

Sometimes the TEMUX device driver behaved erratically, causing interface flaps. No proper PMC-TEMUX error debugs were available that could be collected from the live box in the field without side effects such as line card crashing. This problem has been fixed.

CSCsv55590

When the automatic intercept system (AIS) was injected from the test equipment, the E1 interface reported loss of frame (LOF). This problem has been fixed.

CSCsv73509

For EXEC users under vty configuration mode, when **no aaa new-model** was configured, authentication happened through the local login even though the tacacs login was configured. This problem has been fixed.

CSCsw24700

The Cisco IOS software contained two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSL VPN feature. These vulnerabilities could be be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affected both Cisco IOS WebVPN and Cisco IOS SSL VPN features:

- Crafted HTTPS packet crashed the device.
- SSL VPN sessions caused a memory leak in the device.

This problem has been fixed.

CSCsw27915

Reloading a Cisco 10000 series router with frame-relay traffic shaping, the DLCI command line from the interface disappeared. This problem was observed for Cisco IOS Release 12.0(30)SZ with the frame-relay traffic shaping on. This problem has been fixed.

CSCsw47972

After a Cisco 10000 series router was upgraded from Cisco IOS Release 12.0(28)S5 to Cisco IOS Release 12.0(30)SZ , E1 flaps due to LOF alarms. This problem has been fixed.

CSCsx29123

After a Cisco 10000 series router was upgraded from Cisco IOS Release 12.0(28)S5 to Cisco IOS Release 12.0(30)SZ , E1 flapped due to LOF/RAI alarms. This problem has been fixed.

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