Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.0(30)SZ7

First Published: June, 2008

These release notes provide information about Cisco IOS Release 12.0(30)SZ7 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)SZ7, see the "Caveats for Cisco IOS Release 12.0(30)SZ7" section on page 4.

Cisco IOS Release 12.0(30)SZ7 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)SZ6

To review the release notes for Cisco IOS Release 12.0 S, 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)SZ7:

Supported Hardware

For Cisco IOS Release 12.0(30)SZ7, 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 12.0 S, 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)SZ7 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)SZ7.

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)SZ7 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.

Deferral of 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)SZ7

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats and only select severity 3 caveats are included in the caveats section of this document.

Cisco IOS Release 12.0(30)SZ7 is based on Cisco IOS Release 12.0(30)S5 and Releases 12.0(30)SZ through 12.0(30)SZ6, 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 12.0 S, 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)SZ7:

- Open Caveats in Cisco IOS Release 12.0(30)SZ7, page 4
- Resolved Caveats in Cisco IOS Release 12.0(30)SZ7, page 6

Open Caveats in Cisco IOS Release 12.0(30)SZ7

This section describes caveats that are open in Cisco IOS Release 12.0(30)SZ7.

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 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 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 PPP (MLPPP) interfaces configured, a small PXF buffer leak is observed after a PRE failover. As shown in the following sample output from the **show hardware pxf cpu buffers** command, for buffer pool 3 the total number of buffers (67666) does not equal the number of available buffers (67139). This is observed 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.

CSCsj14143

The ifHCOutOctets and ifHCInOctets values retrieved from the IF-MIB are not correct.

Workaround: No workaround is available.

Resolved Caveats in Cisco IOS Release 12.0(30)SZ7

This section describes caveats that were fixed in Cisco IOS Release 12.0(30)SZ7.

CSCsd17253

The router failed and the following message appeared:

```
MGD timer Next timer has bad reverse linkage, timer = X
```

This symptom was observed on a Cisco 10000 series router running Cisco IOS Release 12.2(13)BZ with a PRE1 installed. The cause of the problem was that the output-command queue from the PXF toward the line cards became full due to high traffic volume. When this occurred, an interrupt generated an alert and attempted to modify the timer associated with the alert, which caused corruption of the timer tree. The router failed because interrupt-generated timer modifications are not allowed. This has been fixed.

CSCse34768

A VRF PIM neighbor was disconnected when the VRF mroute count exceeded the VRF route limit value. This has been fixed.

CSCse56501

A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router cannot trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at:

http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml

CSCsg35077

A device running Cisco IOS software failed when processing an Internet Key Exchange (IKE) message. The device had a valid and complete configuration for IPSec. IPSec virtual private network (VPN) features in Cisco IOS software that use IKE are site-to-site VPN tunnels, EzVPN (server and remote), DMVPN, IPSec over GRE, and GET VPN. This problem was triggered during IKE negotiation when an exchange of messages between IKE peers was necessary. This has been fixed.

CSCsg39295

Password information appeared in a syslog message such as the following:

```
%SYS-5-CONFIG_I: Configured from scp://userid:password@10.1.1.1/config.txt by console
```

This occurred when using SNMP to modify a configuration by using the CISCO-CONFIG-COPY-MIB. The password was exposed in the syslog message when ConfigCopyProtocol of the Service Control Protocol (SCP) or File Transfer Protocol (FTP) was selected. This has been fixed.

CSCsk33054

This is the Cisco Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007 regarding the crash and reload of devices running Cisco IOS after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html

The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html

Preliminary research pointed to a previously known issue that was documented as Cisco bug ID CSCsb08386 (registered customers only), and entitled "PRP crash by show ip bgp regexp", which was already resolved. Further research indicates that the current issue is a different but related vulnerability.

There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

The full text of this response is available at:

http://www.cisco.com/warp/public/707/cisco-sr-20070912-regexp.shtml

CSCsk63208

When the traffic rate was low, the Gigabit Ethernet queue was full, causing latency and packet loss. For example, the output of the **show interface** command indicated the following statistics:

```
Router# show interface gige0/x | include output queue
Output queue 8192/8192, x drops; input queue 0/75, 0 drops
```

This has been fixed.

CSCso63116

The following error message appeared every 60 seconds on a Cisco 10000 series router running Cisco IOS Release 12.0(30)SZ6 with a PRE1 installed:

```
### ASSERTION FAILURE in ../src-4k-c10k/c10k_virtual.c, line 274
<88>
600407C0 60021634 6001F68C 604B9A8C 60470A84
```

This occurred after enabling the following IS-IS configuration on an interface that had MPLS enabled:

```
ip router isis
     isis circuit-type level-1
     isis password isis level-1
     isis csnp-interval 30 level-1
```

This has been fixed.

CSCso98271

Due to a memory leak in the IP-EIGRP(5): PDM process, a Cisco router consumed all available processor memory until memory allocation failure error messages appeared on the console. The router stopped functioning properly and had to be reloaded to recover the memory and restore normal operation. The memory leak was observed when EIGRP was configured on the router. This 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