Release Notes for Cisco 7000 Family for Cisco IOS Release 12.4 XB

June 9, 2008

Cisco IOS Release 12.4(2)XB10

OL-8920-10

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.4(2)XB10. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(2)XB10, see the "Caveats for Cisco IOS Release 12.4 XB" section on page 8 and *Caveats for Cisco IOS Release 12.4*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.4* located on Cisco.com and the Documentation CD-ROM.

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback or go to the following URL to give us your feedback:

http://www.cisco.com/warp/public/732/docsurvey/rtg/ to give us your feedback.

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

This section describes the system requirements for Cisco IOS Release 12.4(2)XB and includes the following sections:

Memory Recommendations

Table 1 Memory Recommendations for the Cisco IOS Release 12.4(2)XB

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	GGSN Standard Feature Set	c7200-g8is-mz	64 MB	512 MB	RAM
		c7200-g8ik9s-mz	64 MB	512 MB	RAM
		c7200-g8ik8s-mz	64 MB	512 MB	RAM

Supported Hardware

Cisco IOS Release 12.4(2)XB supports the following Cisco 7000 platforms:

- Cisco 7200 series routers (including the Cisco 7202, Cisco 7204, and Cisco 7206)
- Cisco 7200 VXR routers (including the Cisco 7204VXR and Cisco 7206VXR)

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 5.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command. The following sample **show version** command output is from a router running a Cisco 7200 series software image with Cisco IOS Release 12.4(2)XB10:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (c7200-g8is-mz), Version 12.4(2)XB10, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, please refer to *How to Choose a Cisco IOS Software Release* at:

http://www.cisco.com/warp/public/130/choosing_ios.shtml

For information about upgrading to a new software release, refer to the appropriate platform-specific document:

Cisco 7200 Series, 7300 Series, 7400 Series, and 7500 Series Routers

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080094c07.shtml

For *Cisco IOS Upgrade Ordering Instructions*, refer to the document at the following location:

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

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. 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 U.S. government regulations. When applicable, the 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.

The feature set tables have been removed from the Cisco IOS Release 12.4 release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

http://www.cisco.com/support/FeatureNav/FNFAQ.html

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.4 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

Step 1 From the Cisco Feature Navigator home page, click **Feature**.

Step 2 To find a feature, use either "Search by full or partial feature name" or "Browse features in alphabetical order." Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the text box on the left side of the web page.

Step 3 Select a feature from the left text box, and click the **Add** button to add a feature to the Selected Features text box on the right side of the web page.

Note To learn more about a feature in the list, click the **Description** button below the left box.

Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.

Step 4 Click **Continue** when you are finished selecting features.

Step 5 From the Major Release drop-down menu, choose **12.4**.

Step 6 From the Release drop-down menu, choose the appropriate maintenance release.

Step 7 From the Platform Family drop-down menu, select the appropriate hardware platform. The "Your selections are supported by the following:" table will list all the software images (feature sets) that support the feature(s) that you selected.

Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.4, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

Step 1 From the Cisco Feature Navigator home page, click **Compare/Release**.

Step 2 In the "Find the features in a specific Cisco IOS release, using one of the following methods:" box, choose **12.4** from the Cisco IOS Major Release drop-down menu.

Step 3 Click **Continue**.

Step 4 From the Release drop-down menu, choose the appropriate maintenance release.

Step 5 From the Platform Family drop-down menu, choose the appropriate hardware platform.

Step 6 From the Feature Set drop-down menu, choose the appropriate feature set. The "Your selections are supported by the following:" table will list all the features that are supported by the feature set (software image) that you selected.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family of routers for Cisco IOS Release 12.4 XB.

New Software Features in Cisco IOS Release 12.4(2)XB10

There are no new software features supported in Cisco IOS Release 12.4(2)XB10.

New Software Features in Cisco IOS Release 12.4(2)XB9

There are no new software features supported in Cisco IOS Release 12.4(2)XB9.

New Hardware Features in Cisco IOS Release 12.4(2)XB9

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB9.

New Software Features in Cisco IOS Release 12.4(2)XB8

There are no new software features supported in Cisco IOS Release 12.4(2)XB8.

New Hardware Features in Cisco IOS Release 12.4(2)XB8

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB8.

New Software Features in Cisco IOS Release 12.4(2)XB7

There are no new software features supported in Cisco IOS Release 12.4(2)XB7.

New Hardware Features in Cisco IOS Release 12.4(2)XB7

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB7.

New Software Features in Cisco IOS Release 12.4(2)XB6

There are no new software features supported in Cisco IOS Release 12.4(2)XB6.

New Hardware Features in Cisco IOS Release 12.4(2)XB6

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB6.

New Software Features in Cisco IOS Release 12.4(2)XB5

There are no new software features supported in Cisco IOS Release 12.4(2)XB5.

New Hardware Features in Cisco IOS Release 12.4(2)XB5

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB5.

New Software Features in Cisco IOS Release 12.4(2)XB4

There are no new software features supported in Cisco IOS Release 12.4(2)XB4.

New Hardware Features in Cisco IOS Release 12.4(2)XB4

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB4.

New Software Features in Cisco IOS Release 12.4(2)XB3

There are no new software features supported in Cisco IOS Release 12.4(2)XB3.

New Hardware Features in Cisco IOS Release 12.4(2)XB3

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB3.

New Software Features in Cisco IOS Release 12.4(2)XB2

There are no new software features supported in Cisco IOS Release 12.4(2)XB2.

New Hardware Features in Cisco IOS Release 12.4(2)XB2

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB2.

New Software Features in Cisco IOS Release 12.4(2)XB1

There are no new software features supported in Cisco IOS Release 12.4(2)XB1.

New Hardware Features in Cisco IOS Release 12.4(2)XB1

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB1.

New Software Features in Cisco IOS Release 12.4(2)XB

The following new software feature is supported by in Cisco IOS Release 12.4(2)XB:

Proxy Call Session Control Function (P-CSCF) Discovery

This release of Cisco GGSN Release 6.0 provides support for the Proxy Call Session Control Function (P-CSCF) Discovery feature.

For information about the features in GGSN Release 6.0, see the Cisco IOS Release 12.4(2)XB Cisco GGSN Release 6.0 configuration guide and command reference at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xb2/index.htm

New Hardware Features in Cisco IOS Release 12.4(2)XB

There are no new hardware features supported in Cisco IOS Release 12.4(2)XB.

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Important Notes for Cisco IOS Release 12.4 XB

This section describes important notes related to Cisco IOS Release 12.4 XB.

Important Notes for Cisco IOS Release 12.4(2)XB2

This section describes important notes related to Cisco IOS Release 12.4(2)XB2:

- The ISA card (IPsec card for 7200) is no longer supported.

Caveats for Cisco IOS Release 12.4 XB

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 document.

This section contains only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.4 and Cisco IOS Release 12.4 T are also in Cisco IOS Release 12.4(2)XB10.

For information on caveats in Cisco IOS Release 12.4, see *Caveats for Cisco IOS Release 12.4*.

For information on caveats in Cisco IOS Release 12.4 T, see *Caveats for Cisco IOS Release 12.4 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

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 Mainline> Troubleshoot and Alerts > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may 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.)

Table 2 Caveats Reference for Cisco IOS Release 12.4 XB

DDTS Number	Open in Release	Resolved in Release
CSCec12299		12.4(2)XB6
CSCeh69873		12.4(2)XB
CSCei37916		12.4(2)XB2
CSCei59800		12.4(2)XB3
CSCei87444	12.4(2)XB1 12.4(2)XB2	
CSCej09790		12.4(2)XB1
CSCej20505		12.4(2)XB5

Table 2 Caveats Reference for Cisco IOS Release 12.4 XB (continued)

CSCej21472	12.4(2)XB1 12.4(2)XB3 12.4(2)XB4 12.2(2)X5	
CSCej48454		12.4(2)XB1
CSCej48745		12.4(2)XB
CSCej48899		12.4(2)XB
CSCej72003		12.4(2)XB
CSCej79360		12.4(2)XB1
CSCej85613		12.4(2)XB1
CSCek26492		12.4(2)XB2
CSCek28967		12.4(2)XB2
CSCek32859		12.4(2)XB2
CSCek43456		12.4(2)XB3
CSCin95836		12.4(2)XB6
CSCin98692	12.4(2)XB1	12.4(2)XB2
CSCin99848		12.4(2)XB3
CSCin99862		12.4(2)XB5
CSCir02107		12.4(2)XB7
CSCir00690		12.4(2)XB5
CSCir00864		12.4(2)XB5
CSCir01528		12.4(2)XB6
CSCsa85015	12.4(2)XB	12.4(2)XB1
CSCsb25337		12.4(2)XB2
CSCsb84438		12.4(2)XB
CSCsb94067	12.4(2)XB	12.4(2)XB1
CSCsb96863		12.4(2)XB1
CSCsc05462		12.4(2)XB
CSCsc06275	12.4(2)XB	
CSCsc09233	12.4(2)XB	12.4(2)XB2
CSCsc11366	12.4(2)XB1	
CSCsc12583	12.4(2)XB1	12.4(2)XB2
CSCsc19635		12.4(2)XB1
CSCsc25722		12.4(2)XB
CSCsc31776		12.4(2)XB
CSCsc49575	12.4(2)XB1	
CSCsc58186		12.4(2)XB1
CSCsc60231	12.4(2)XB1	

Table 2 Caveats Reference for Cisco IOS Release 12.4 XB (continued)

CSCsd95616		12.4(2)XB6
CSCsc65387		12.4(2)XB1
CSCsc86028		12.4(2)XB1
CSCsc94608	12.4(2)XB1	
CSCsd40334		12.4(2)XB2
CSCsd58381		12.4(2)XB2
CSCsd66755		12.4(2)XB2
CSCsd80775		12.4(2)XB2
CSCsd81407		12.4(2)XB6
CSCse05642		12.4(2)XB3
CSCse12345	12.4(2)XB2	12.4(2)XB3
CSCse50873		12.4(2)XB3
CSCse56501		12.4(2)XB6
CSCse62599		12.4(2)XB3
CSCse64581		12.4(2)XB3
CSCse68138		12.4(2)XB3
CSCse68355		12.4(2)XB6
CSCsf04754		12.4(2)XB3
CSCsf13403		12.4(2)XB5
CSCsf18925		12.4(2)XB6
CSCsf30058		12.4(2)XB5
CSCsf96125		12.4(2)XB8
CSCsf97873		12.4(2)XB9
CSCsg16908		12.4(2)XB5
CSCsg18574		12.4(2)XB6
CSCsg83347		12.4(2)XB6
CSCsg91306		12.4(2)XB8
CSCsg91326		12.4(2)XB6
CSCsg94642		12.4(2)XB6
CSCsh21101		12.4(2)XB5
CSCsh87457		12.4(2)XB6
CSCsh97579		12.4(2)XB6
CSCsi01470		12.4(2)XB6
CSCsi60004		12.4(2)XB6
CSCsi80749		12.4(2)XB6
CSCsj40311		12.4(2)XB6
CSCsj74145		12.4(2)XB6

Table 2 Caveats Reference for Cisco IOS Release 12.4 XB (continued)

CSCsj85065		12.4(2)XB10
CSCsk29283		12.4(2)XB7
CSCsk42759		12.4(2)XB10
CSCsk62253		12.4(2)XB10
CSCsk73104		12.4(2)XB8
CSCsk94202		12.4(2)XB8
CSCsl62609		12.4(2)XB10
CSCsm42890		12.4(2)XB9

Open Caveats—Cisco IOS Release 12.4(2)XB10

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB10 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.4(2)XB10.

Resolved Caveats—Cisco IOS Release 12.4(2)XB10

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB10. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsl62609

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsk42759

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsj85065

A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml.

- CSCsk62253

  Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

  1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
  2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

Open Caveats—Cisco IOS Release 12.4(2)XB9

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB9 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.4(2)XB9.

Resolved Caveats—Cisco IOS Release 12.4(2)XB9

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB9. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsf97873

  A Cisco Gateway GPRS Support Node (GGSN) using the **ppp regen apn** command to create a Layer 2 Tunnel Protocol (L2TP) tunnel from the GGSN to the L2TP Network Server (LNS) is inconsistent in its handling of the Time to Live (TTL) value for the uplink and downlink.

  This discrepancy occurs under the following scenarios:

  MSclient----SGSN----GTP-----GGSN------L2TP-----LNS

  MS-Client sends ICMP packet with ICMP data of 1432 bytes: Scenario 1, no IP fragmentation
  MS-Client sends ICMP packet with ICMP data of 1433 bytes: Scenario 2, IP fragmentation

  In the uplink direction (SGSN--->GGSN--->LNS), the TTL value of the packet is always 128 for Scenario 1 and 2. The TTL is not decreased at the GGSN.

  In the downlink direction (LNS---->GGSN---->SGSN), the behavior differs for Scenario 1 and 2.

  In Scenario 1, the TTL value is decreased by 1 by the GGSN, and no IP fragmentation occurs.

  In Scenario 2, the TTL is not changed by the GGSN and remains the same. As a result, when the packet of Scenario 2 gets into the GPRS Tunneling Protocol (GTP) or L2TP tunnel, the total packet size is 1501 bytes, and the packet must be fragmented by the tunnel endpoints (SGSN/GGSN/LNS).

Protocol header calculation: GTP: IP (20)+UDP(8)+GTP(12)+IP(20)+ICMP Header(8)=68 byte L2TP: IP (20)+UDP(8)+L2TP(8)+PPP(4)+IP(20)+ICMP Header(8)=68 Byte

There are no known workarounds.

- CSCsm42890

  An input queue wedge can occur on the GTP Virtual Access interface of a Cisco processor running Gateway GPRS Support Node (GGSN) preventing data traffic for the affected APNs.

  This condition occurs only if the access point name (APN) is configured with the redirect-all feature and if the mobile sends upstream packets with the Time To Live (TTL) option in the IP header set to 1.

  Workaround: Unconfigure the access-point, or configure an access control list (ACL) with drop for packets with TTL equal to 1.

Open Caveats—Cisco IOS Release 12.4(2)XB8

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB8 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.4(2)XB8.

Resolved Caveats—Cisco IOS Release 12.4(2)XB8

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB8. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsf96125

  The Cisco Gateway GPRS Support node (GGSN) does not decrement the time-to-live (TTL) value before sending the packet towards the Gigabit interface.

  This condition occurs when the IP packet is fragmented. If the IP packet is not fragmented, the GGSN decrements the TTL by 1 to 127 before sending it out to the Gigabit interface.

  Workaround: Avoid fragmentation by conforming to the maximum transmission unit (MTU) sizes between Mobile Station and GGSN.

- CSCsg91306

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml.

- CSCsk73104

  Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

  Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml

- CSCsk94202

  The Cisco Gateway GPRS Support node (GGSN) reloads when data is sent through a packet data protocol (PDP) context and the PDP context is deleted at the same time.

  This condition can occur under certain timing conditions involving data transfer and PDP deletion events.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(2)XB7

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB7 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.4(2)XB7.

Resolved Caveats—Cisco IOS Release 12.4(2)XB7

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB7. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCir02107

  On a Cisco router running the Cisco Gateway GPRS Support node (GGSN) software, when a path is created without a recovery IE being received from the Serving GPRS support node (SGSN), and the path is later updated with a valid recovery IE, the standby GGSN does not update the recovery IE with this new value.

  This condition occurs only if the SGSN is incapable of sending a recovery IE in the create request.

  Workaround: Ensure the first message from the SGSN for a new path includes the recovery IE as described in the 3GPP specification 29.060 section 7.3.1.

- CSCsk29283

  On a Cisco Multiprocessor WAN Application Module (MWAM) running the Cisco Gateway GPRS Support node (GGSN) software, if the Serving GPRS support node (SGSN) does not include a recovery IE in the initial signaling requests and then a recovery IE is included subsequent signaling requests, the GGSN initiates a path cleanup for the path recovery changed and deletes all existing PDPs on the path.

  Workarounds: 1. Enable echo requests on the GGSN. When echo requests are enabled, the GGSN will always have the current recovery IE of the SGSN because the recovery IE is included in the echo response. 2. If possible, set the SGSN to include the recovery IE in all signaling messages.

Open Caveats—Cisco IOS Release 12.4(2)XB6

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB6 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.4(2)XB6.

Resolved Caveats—Cisco IOS Release 12.4(2)XB6

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates 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-20080924-vpn.shtml.

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

- CSCir01528

  On a Cisco router running the Cisco Gateway GPRS Support node (GGSN) software, and configured to allocate IP addresses from a RADIUS for an access point name (APN), an incorrect syslog message might be printed when the RADIUS server does not return an IP address for a particular user. The message incorrectly says that no RADIUS server is available.

  Workaround: The customer can safely ignore this message.

- CSCsd81407

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates 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-20080924-multicast.shtml.

- 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 can not 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.

- CSCse68355

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsf18925

  A Multiprocessor WAN Application Module (MWAM) running the Cisco Gateway GPRS support node (GGSN) might reload while doing multiple Simple Network Management Protocol (SNMP) operations on a service-aware access point name (APN). This crash is a rare occurrence.

  There are no known workarounds.

- CSCsg18574

  A few issues exist with the way the Gateway GPRS support node (GGSN) security feature is working when Cisco Express Forwarding (CEF) is enabled (**ip cef** command) or in the process path:

  3. Source address verification

     When CEF is enabled (**ip cef** command), the cef_drop, rcv_pkt_count, and rcv_bytes_count counters are not incremented in the **show gprs gtp pdp tid** command output. In addition, the corresponding counters, which reflect the quantities the GGSN receives from the Serving GPRS support node (SGSN), are not incremented in the **show gprs access-point** and **show gprs gtp statistics** commands.

     When CEF is disabled (**no ip cef** command), and source address verification is enabled, the user is charged for dropped packets. In addition, for GPRS Tunneling Protocol Version 1 (GTPv1) packet data protocol (PDP) contexts, the byte count displays incorrectly. For example, when 70 bytes of data are sent, the **show gprs pdp tid** and **show gprs access-point statistics** commands display the byte count as 74.

  4. Destination address verification

     When CEF is enabled (**ip cef** command), the user is not charged for dropped packets when they should be. In addition, the cef_drop, rcv_pkt_count, and rcv_bytes_count counters are not incremented in the **show gprs gtp pdp tid** command output, and the corresponding counters, which reflect the quantities the GGSN receives from the SGSN, are not incremented in the **show gprs access-point** and **show gprs gtp statistics** commands.

When CEF is disabled (**no ip cef** command) for GTPv1 PDP contexts, the byte count displays incorrectly. For example, when 70 bytes of data are sent, the **show gprs pdp tid** and **show gprs access-point statistics** commands display the byte count as 74.

There are no known workarounds.

- CSCsg83347

  The cgprsAccPtName and cgprsAccPtMsIsdnSuppressedValue objects may not accept a null string.

  There are no known workarounds.

- CSCsg91326

  When the Diameter server experiences delays in responses and the Cisco Gateway GPRS support node (GGSN) keeps generating new authorization requests, the Gi0/0 interface on a Multiprocessor WAN Application Module (MWAM) shows the input queue size increase to the maximum value.As a result, the GGSN encounters a path failure to the Serving GPRS support node (SGSN) and active PDPs are deleted.

  There are no known workarounds.

- CSCsg94642

  The following Simple Network Management Protocol (SNMP) MIBS are not functioning properly:

  - cgprsAccPtRevUpstreamTrafficVol.4 = 1339050544120284
  - cgprsAccPtRevDownstrTrafficVol.4 = 5272506148764497

  There are no known workarounds.

- CSCsh87457

  After setting cgprsAccPtName to null through the Simple Network Management Protocol (SNMP), the following conditions can occur:

  - The access point name (APN) name might display with some junk characters in the running configuration.
  - The Gateway GPRS support node (GGSN) might reload when you attempt to change the APN name through the CLI.

  Workaround: Set the APN name using the CLI.

- 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.

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

- CSCsi60004

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsi80749

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsj40311

  A Cisco router running the Cisco Gateway GPRS support node (GGSN) software might reload when a create PDP context request is received with an extension header to the GPRS Tunneling Protocol (GTP) header and the extension header has a length of 0 bytes.

  Workaround: Verify the Serving GPRS support node (SGSN) includes a correct GTP header with an accurate length for the extension headers, if any are used. If these values are incorrect, configure them so that they are correct. (Most SGSNs do not support extension headers and, if they do, they should not use a 0 byte length.)

- CSCsj74145

  On a Cisco Multiprocessor WAN Application Module (MWAM) running the Cisco Gateway GPRS support node (GGSN) software, if an Error-Indication is received from the Serving GPRS support node (SGSN) on a GPRS Tunneling Protocol Version 1 (GTPv1) path, which leads to packet data protocol (PDP) context deletion on the GGSN, the corresponding Accounting-Stop shows the Acct-Terminate-Cause as "Unknown," instead of "Nas-Error." If the SGSN path is GTPv0, the Acct-Terminate-Cause would be "Nas-Error."

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(2)XB5

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCej21472

  In Cisco IOS GGSN Release 6.0, when an extended quality of service (QoS) profile is sent to the Gateway GPRS support node (GGSN), the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for extended maximum and guaranteed bit rates for downlink.

  This condition occurs only when an extended QoS IE is sent in a packet data protocol (PDP) create request.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(2)XB5

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCej20505

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCin99862

  A Cisco Gateway GPRS support node (GGSN) displays duplicate entries for the packet data protocol (PDP) context when the **show gprs gtp pdp-context all** and the **show gprs gtp pdp-context ms-address** commands are executed.

  This issue occurs for both the V0 and V1 types of PDP context. The problem has not been reported in Cisco IOS releases 12.4(2)XB2, 12.4(XB)4, or 12.3(14)YQ.

  There are no known workarounds.

- CSCir00690

  When the Cisco Gateway GPRS support node (GGSN) sends Diameter packets that include a radio access technology (RAT) value, the M-bit is not set in the CCR-I message, although it should be.

  There are no known workarounds.

- CSCir00864

  A Cisco Gateway GPRS Support Node (GGSN) running version R6.0 encodes an IPv4 Proxy Call Session Control Function (P-CSCF) address as an IPv4 container inside the Protocol Control Option (PCO) information element (IE). According to TS 24.008, the Cisco GGSN should encode an IPv4 P-CSCF address as an IPv6 mapped address (defined in RFC 2373).

  There are no known workarounds.

- CSCsf13403

  Spurious memory access occurs when the **encapsulation gtp** command is configured under the virtual template. In addition, the configuration specified with the **gprs access-point-list** command might not take effect.

  There are no known workarounds.

- CSCsf30058

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's file system, including the device's saved configuration, which may include passwords or other sensitive information.

  The Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the Cisco IOS FTP Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

- CSCsh21101

  The Cisco Gateway GPRS serving node (GGSN) does not take into account the elapsed time when it reclaims an IP address that is still in the “hold” state.

  This issue occurs when the Dynamic Host Configuration Protocol (DHCP) is allocating an IP address and the session is torn down and brought up again at least 2 to 3 times just before the renewal.

  Workaround: Increase the lease time on the DHCP server.

Open Caveats—Cisco IOS Release 12.4(2)XB4

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCej21472

  In Cisco IOS GGSN Release 6.0, when an extended quality of service (QoS) profile is sent to the Gateway GPRS support node (GGSN), the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for extended maximum and guaranteed bit rates for downlink.

  This condition occurs only when an extended QoS IE is sent in a packet data protocol (PDP) create request.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(2)XB4

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.4(2)XB4.

Open Caveats—Cisco IOS Release 12.4(2)XB3

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCej21472

  In Cisco IOS GGSN Release 6.0, when an extended quality of service (QoS) profile is sent to the Gateway GPRS support node (GGSN), the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for extended maximum and guaranteed bit rates for downlink.

  This condition occurs only when an extended QoS IE is sent in a packet data protocol (PDP) create request.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(2)XB3

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei59800

  The **commands configure include all policy-map** CLI view command does not include the **policy-map mode** commands as part of the view.

  There are no known workarounds.

- CSCek43456

  When a Gateway GPRS support node (GGSN) sends the GGSN-call detail record (G-CDR), it includes the quality of service (QoS) profile IE, but one octet is added at the end of the field.

  This condition occurs when the GGSN receives the QoS profile IE from the Serving GPRS support node (SGSN) in the packet data protocol (PDP) create request, and the length of the field is 12 octets. The QoS profile encoded by GGSN in the G-CDR has one octet added at the end of the field.

  There are no known workarounds.

- CSCin99848

  A Cisco Gateway GPRS support node (GGSN) running the R7.0 image is not able to lookup the packet data protocol (PDP) context correctly when the Server Load Balancing (SLB) PDP status query contains an nsapi value between 0 and 4.

  There are no known workarounds.

- CSCse05642

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCse12345

  In a Cisco Gateway GPRS support node (GGSN), when a radio access technology (RAT) field is provided in the create/update packet data protocol (PDP) request, the value encoded in the RADIUS Access-Request and Accounting-Request packets is the incorrect length.

  This condition occurs when a RAT field is provided in a create/update PDP request.

  There are no known workarounds.

- CSCse50873

  When GPRS Tunneling Protocol Version 1 (GTPv1) is used, quality of service (QoS) displays all zeros in the **show gprs gtp pdp-context** command.

  This condition occurs with GTPv1 only.

  Workaround: Condition does not affect performance; display issue only.

- CSCse62599

  A Cisco Gateway GPRS support node (GGSN) does a reload when rare passwords are used.

  This condition occurs when the create request is using the Virtual Access Point Name (APN) feature only, and the password has the @ character in the password.

  Workaround: Do not use the Virtual Access Point Name feature to get the real APN name using the username@<domain>. Use the pre-authenticate Virtual APN feature instead to get this information.

- CSCse64581

  A Cisco Gateway GPRS support node (GGSN) running a R5.x/R6.0 image reloads when a secondary create packet data protocol (PDP) context comes with a traffic flow template (TFT) having a TFT code of “No TFT operation” and the packet has some filter in it.

  This condition occurs only when **debug gprs gtp parsing** is enabled.

  There are no known workarounds.

- CSCse68138

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

Open Caveats—Cisco IOS Release 12.4(2)XB2

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei87444

  A Cisco Gateway GPRS support node (GGSN) with an encrypted image reloads when it has a heavy load.

  This condition occurs when CPU usage is consistently over 96% for a long timeframe and the router is sending bi-directional data over all the IPSec tunnels at the same, causing the IPSec card to reset.

  Workaround: Configure Policing such that high unchecked data is not sent for long periods of time.

- CSCse12345

  In Cisco Gateway GPRS support node (GGSN), when a radio access technology (RAT) field is provided in the create/update packet data protocol (PDP) request, the value encoded in the RADIUS Access-Request and Accounting-Request packets is the incorrect length.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(2)XB2

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei37916

  A Cisco Gateway GPRS support node (GGSN) running Cisco IOS Release 12.4 and GGSN Release 5.2 does not function properly when wait-accounting and authentication, authorization, and accounting (AAA) Broadcast Accounting are configured on an access point name (APN). When the first RADIUS server responds to an Accounting Start message, the GGSN establishes the packet data protocol (PDP) context without waiting for responses from all other RADIUS servers. Under a stress condition, the GGSN may reload.

  This condition occurs only when both wait-accounting and AAA Broadcast Accounting are configured together on an APN.

  There are no known workarounds.

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCek28967

  In a Cisco Gateway GPRS support node (GGSN) running Cisco IOS Release 12.4(2)XB, the packet data protocol (PDP) create request is rejected under the following scenario: octet 9 of the quality of service (QoS) IE has a value of less than FE, and the extended QoS header (octet 15 and 16) are present.

  Workaround: The PDP create request should not have the extended QoS IE if the required bandwidth is less than 8640 Kbps (or octet 9 of the QoS IE has a lesser value than FE).

- CSCek32859

  In Cisco IOS GGSN Release 12.4(2)XB, the Gateway GPRS support node (GGSN) does not accept the **gprs gtp map signalling tos** command.

  There are no known workarounds.

- CSCin98692

  A Cisco Gateway GPRS support node (GGSN) reloads on executing the **show aaa attribute protocol radius** command.

  This condition occurs only when this command is executed from the Command Line Interface.

  There are no known workarounds. Ideally, one should not be even executing this command because the supported attributes list is already given in the RADIUS White Paper.

- CSCsb25337

  Cisco devices running Cisco IOS, which support voice and are not configured for Session Initiated Protocol (SIP) are vulnerable to a crash under yet to be determined conditions, but isolated to traffic destined to User Datagram Protocol (UDP) 5060. SIP is enabled by default on all Advanced images which support voice and do not contain the fix for CSCsb25337. Devices which are properly configured for SIP processing are not vulnerable to this issue. Workarounds exist to mitigate the effects of this problem. This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml

- CSCsc09233

  The cGgsnSlbNotif retains the previous value even if the corresponding configuration is removed using a **no** CLI from the Gateway GPRS support node (GGSN).

  There are no known workarounds.

- CSCsc12583

  The Gateway GPRS support node (GGSN) reloads under control and data traffic stress condition.

  This condition occurs when consecutive actions of create and delete requests for a large number packet data protocol (PDP) contexts are at a very high rate, especially when there is not sufficient time for all the contexts to be established or cleaned up properly.

  There are no known workarounds.

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd58381

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd66755

  In Cisco Gateway GPRS support node (GGSN), when Interim Accounting is not configured, the updated values of the Serving GPRS support node (SGSN) address and QoS Negotiated do not appear in the Accounting-Stop message.

  This condition occurs under the following scenario:

  1. Interim Accounting is not configured under the access point name (APN).

  2. A GPRS Tunneling Protocol Version 1 (GTPv1) packet data protocol (PDP) is created.

  3. An Update request is received with a new SGSN Address or QoS Negotiated value.

  4. The PDP is deleted.

  5. The corresponding Accounting-Stop still has the SGSN Address and QoS Negotiated values received in the create request.

  Workaround: Enable Interim Accounting under the APN.

- CSCsd80775

  The Cisco Gateway GPRS support node (GGSN) sends a wrong Message-length value for Password Authentication Protocol (PAP) Authenticate-Ack frames inside Create PDP Context Response messages. The Data field inside the Authenticate-Ack frame contains a one-byte Msg-Length subfield that specifies the length of the Message subfield that follows it. The Message subfield contains an arbitrary string of data whose use is implementation dependent. It may be used to provide an indication of authentication success or failure to the user. If not used, the Msg-Length field is still included, but its value is set to zero. When looking into a sniffer trace you can see that Msg-Length subfield has not been included in the frame, and the incorrect value of Msg-Length equal to 65 (0x41) is the first letter (letter “A”) in the message “Authentication successful.”

  This condition occurs when setting a message in the Message Field of PPP PAP. While this issue does not have an operational impact, as PAP authentication passes successfully, it can cause monitoring issues.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(2)XB1

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei87444

  A Cisco Gateway GPRS support node (GGSN) with an encrypted image reloads when it has a heavy load.

  This condition occurs only when CPU usage is consistently over 96% for a long timeframe and the router is sending bi-directional data over all the IPSec tunnels at the same time, causing the IPSec card to reset.

  Workaround: Configure policing such that high unchecked data is not sent for long periods of time.

- CSCej21472

  In Cisco IOS GGSN Release 6.0, when an extended quality of service (QoS) profile is sent to the Gateway GPRS support node (GGSN), the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for extended maximum and guaranteed bit rates for downlink.

  This condition only occurs when an extended QoS IE is sent in a packet data protocol (PDP) create request.

  There are no known workarounds.

- CSCin98692

  A Cisco Gateway GPRS support node (GGSN) reloads on executing the **show aaa attribute protocol radius** command.

  This condition occurs only when this command is executed from the Command Line Interface.

  There are no known workarounds. Ideally, one should not be executing this command because the supported attributes list is already given in the RADIUS White Paper.

- CSCsc11366

  A Cisco Gateway GPRS support node (GGSN) experiences a delay in sending call detail records (CDRs) when a node alive message comes from the charging gateway to the GGSN.

  This condition occurs only when the charging gateway has been marked as Down in the GGSN and then a node alive is received.

  There are no known workarounds.

- CSCsc12583

  The Gateway GPRS support node (GGSN) reloads under control and data traffic stress condition.

  This condition occurs when consecutive actions of create and delete requests for a large number packet data protocol (PDP) contexts are at a very high rate, especially when there is not sufficient time for all the contexts to be established or cleaned up properly.

  There are no known workarounds.

- CSCsc49575

  The cGgsnSANotifCsgRealAddress value is 0.0.0.0 when cGgsnSACsgStateDownNotif or cGgsnSACsgStateUpNotif traps are generated.

  There are no known workarounds.

- CSCsc60231

  A Cisco Gateway GPRS support node (GGSN) running R6.0 generates traceback when trying to create a packet data protocol (PDP) if the bandwidth was not configured in the **gprs qos bandwidth-pool** command.

  This condition occurs only when **debug gprs gtp event** is enabled and the bandwidth pool does not have bandwidth configured.

  Workaround: Do not switch on the **debug gprs gtp even**t.

- CSCsc94608

  In a Cisco Mobile Exchange (CMX) environment, the Content Services Gateway (CSG) is configured to send a RADIUS packet of Disconnect packets to the Gateway GPRS support node (GGSN) upon receiving a User Disconnect request from the Quota Server. The CSG is configured to report 3GPP IMSI (26/10415/1) and NSAPI (26/10415/10) in the Packet of Disconnect (PoD) message. However, when the CSG sends the PoD, the GGSN reports an unsupported attribute and vendor-specific attribute (VSA) format error, drops the PoD request, and doesn't delete the packet data protocol (PDP) context.

  This condition occurs when the CSG is configured to report 3GPP IMSI and NSAPI in the RADIUS PoD. When sub-attributes are used, the CSG encodes them in a single VSA. If the CSG is configured to send RADIUS Accounting Session Id in the PoD message instead of IMSI+NSAPI, then the GGSN accepts the message, deletes the PDP context, and this condition does not occur.

  Workaround: In the CMX environment, configure the CSG to report the RADIUS Accounting Session Id in the PoD message for the Packet of Disconnect feature.

Resolved Caveats—Cisco IOS Release 12.4(2)XB1

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCej09790

  In a Cisco Gateway GPRS support node (GGSN), when a Secondary packet data protocol (PDP) context is created, it always has a Charging Characteristic Selection Mode value of “subscriptionSpecific”. But actually, “subscriptionSpecific” is a value only used when the Charging Characteristics is assigned by authentication, authorization, and accounting (AAA).

  The secondary PDP should reflect the same charging characteristics value that is used by the primary PDP.

  There are no known workarounds.

- CSCej48454

  The Gateway GPRS support node (GGSN) interface inputq loses communications.

  This condition occurs under the following scenarios:

  - The access point name (APN) redirect all feature needs to be enabled
  - The GGSN receive user payload packet is aimed to an internal loopback address
  - The packet size is less than 1500
  - The packet needs to include something that can not be Cisco Express Forwarding (CEF) switched, for example, ip option

  Workaround: Use config APN ACL to deny any user payload traffic that is aimed to an internal loopback address.

- CSCej79360

  The Transmission Control Protocol (TCP) path between a charging gateway and a Cisco Gateway GPRS support node (GGSN) is flapping.

  This condition occurs in the following scenario:

  - Redirect all is enabled in GGSN.
  - Many redirect all traffic needs to punt to process level because there is an ip option field in the packet.
  - The charging path is TCP.

  This condition occurs because the GGSN sends 128 charging msg simultaneously, but the TCP send window is only 20K bytes, and as a result, many of the packet are dropped before getting out of the GGSN. After max retry and no response, the GGSN marks the charging gateway as down.

  Workaround: Reduce the number of messages that are sent simultaneously to less than 20 if TCP is used. This will make the charging msg send slower but more reliable.

- CSCej85613

  A Cisco router running Gateway GPRS support node (GGSN) software cannot send Cisco Express Forwarding (CEF) switched packets.

  This condition occur s only when downstream packets are being sent to the GGSN, the GGSN reports no adjacency is set up, and the packets are process switched.

  Workaround: Disable CEF on the GGSN (use the **no ip cef** command in global configuration mode), and then re-enable CEF (use the **ip cef** command in global configuration mode).

  This workaround will prevent packet drops until the next reload. If GGSN is reloaded, then disable/enable CEF again.

- CSCsa85015

  A traceback indicating bad refcounf occurs on the Gateway GPRS support node (GGSN). There is no service impact, and this traceback does not cause any other side effects.

  This condition occurs under the following scenario:

  - The redirect all feature is enabled.
  - The GPRS Tunneling Protocol (GTP) payload packet is not an IP packet or it is a wrongly formatted IP packet.

  Workaround: Do not enable the redirect all feature.

- CSCsb94067

  A Simple Network Management Protocol (SNMP) query on cgprsAccPtSecNetbiosServer returns the following error message:

  ```
  Packet too big
  ```

  There are no known workarounds.

- CSCsb96863

  When a CCR (Update) is sent as a result of a Service-Auth message from the Content Services Gateway (CSG for a category that was previously IDLE, it contains the Reporting-Reason attribute. This attribute should not be present unless usage is being reported in a CCR message.

  There are no known workarounds.

- CSCsc19635

  A Cisco Gateway GPRS support node (GGSN) reloads.

  This condition occurs when the GGSN and the charging gateway are wrongly configured, such as when GGSN is configured for the protocol using the Long Header and the charging gateway is configured for the protocol using the Short Header.

  Workaround: Configure the charging gateway header properly. If the charging gateway is using the Short Header, then the GGSN should also be configured accordingly.

- CSCsc58186

  Gateway GPRS support node (GGSN) Call Admission Control may not work with extended quality of service (QoS).

  There are no known workarounds.

- CSCsc65387

  When packet data protocol (PDP) create fails on a Gateway GPRS support node (GGSN) due to the Call Admission Control (CAC) policy resource limit being reached, and Server Load Balancing (SLB) fails on its maximum reassign attempts to other GGSNs, the expected create response failure with cause 199 (NO RESOURCE) is not sent to the Serving GPRS support node (SGSN). This error occurs because of an incorrect sequence number in the CAC reassign notification message from the GGSN to the SLB.

  This condition occurs when all the GGSNs attempted by the SLB have run out of resources for the access point name (APN), as defined by the CAC policy.

  There are no known workarounds. However, this issue can be solved by allocating/deploying more resources to the GGSNs.

- CSCsc86028

  A Cisco Gateway GPRS support node (GGSN) running the R6.0 image does not display conditional msisdn debugs after the packet data protocol (PDP) is deleted and created again. The debugs are displayed only the first time.

  This condition occurs when the PDP is deleted and recreated again with the same msisdn.

  Workaround: Unconfigure and re-configure the conditional msisdn debug.

Open Caveats—Cisco IOS Release 12.4(2)XB

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsa85015

  A traceback indicating bad refcounf occurs on the Gateway GPRS support node (GGSN). There is no service impact and this traceback does not cause any other side effects.

  This condition occurs under the following scenario:

  1. The redirect all feature is enable.

  2. The GPRS Tunneling Protocol (GTP) payload packet is not an IP packet or it is a wrongly-formatted IP packet.

  Workaround: Do not enable the redirect all feature.

- CSCsb94067

  A Simple Network Management Protocol (SNMP) query on cgprsAccPtSecNetbiosServer returns the following error message:

  ```
  Packet too big
  ```

  There are no known workarounds.

- CSCsc06275

  The **mode** option is not available in the **no gprs slb** command.

  Workaround: Use the MIB object cGgsnSlbMode to set it to directed(1) or dispatched(2).

- CSCsc09233

  The cGgsnSlbNotif retains the previous value even if the corresponding configuration is removed using the **no** CLI from the Gateway GPRS support node (GGSN).

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(2)XB

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(2)XB. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeh69873

  When a Gateway GPRS support node (GGSN) receives packet data protocol (PDP) context with non-real time traffic classes and the Service Selection Dashboard (SSD) value is not 1 (that is, speech), the PDP is rejected.

  This condition occurs because CR-830 is not compliant. To be compliant with CR-830, accept PDP context with non-real time classes for any value of SSD.

  There are no known workarounds.

- CSCej48745

  The data volume content is wrong when the radio access technology (RAT) change causes the call detail record (CDR) to be closed.

  This condition occurs when a RAT change in packet data protocol (PDP) is updated.

  There are no known workarounds.

- CSCej48899

  In a Cisco Gateway GPRS support node (GGSN) running Cisco IOS Release 12.4(2)XB, there are several record closure containers within one call detail record (CDR). This issue occurs when an update request occurs more than once with the radio access technology (RAT) and newly supported IEs are being changed. The trigger does not reset the values, so the values are repeated.

  There are no known workarounds.

- CSCej72003

  A Cisco Gateway GPRS support node (GGSN) running Cisco IOS Release 12.4(2)XB, sends negative data volume in the call detail record (CDR) under the following conditions:

  - The charging profile is configured under the access point name (APN) with no reset for triggers.
  - If there is a Serving GPRS support node (SGSN) change, radio access technology (RAT) change, and quality of service (QoS) change all occurring at the same instant that the Data volume sent in the CDR is negative.

  There are no known workarounds.

- CSCsb84438

  A Cisco router running Gateway GPRS support node (GGSN) software unexpectedly reloads if the following conditions persist for a long time:

  1. The Dynamic Host Configuration Protocol (DHCP) server is very slow.

  2. The user session activation is high.

  3. The DHCP lease is very short.

  In some stress error conditions, GGSN enqueues an already free element into queue.

  Workaround: Use a faster DHCP server or configure a longer DHCP lease time in the DHCP server.

- CSCsc05462

  In Cisco IOS Release 12.3(14)YQ3 (Cisco GGSN Release 5.2), a simultaneous Public Land Mobile Network (PLMN) and quality of service (QoS) change can cause a duplicated volume report. The same byte counts are reported in successive containers; one count is added for record closure because of the PLMN change, and the other count is added because of the QoS change.

  This condition occurs only when no charging profile was configured under the access point name (APN) (that is, when the default charging profile is used).

  Workaround: Use an APN-specific charging profile.

- CSCsc25722

  In a Cisco Gateway GPRS support node (GGSN) running Cisco IOS Release 12.4(2)XB, the Authentication Fail trap is not sent if there is an incorrect username or password.

  There are no known workarounds.

- CSCsc31776

  In Cisco IOS Gateway GPRS support node (GGSN) Releases 5.0 and 6.0, the router unexpectedly reloads after about 3000 create packet data protocol (PDP) context requests are sent and the following configurations exist:

  1. The **debug gprs gtp message** command is configured.

  2. An external Dynamic Host Configuration Protocol (DHCP) IP address assignment is configured.

  3. VPN routing and forwarding (VRF) is configured on the access point name (APN), but not on the DHCP server.

  There are no known workarounds.

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family of routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 37
- Platform-Specific Documents, page 38
- Feature Modules, page 39

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.4 and Cisco IOS Release 12.4T and are located on Cisco.com and http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.4*

  On Cisco.com at:

  Products and Services > Cisco IOS Software >Cisco IOS Release 12.4>General Information>Release Notes> Cross-Platform Release Notes

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software> Cisco IOS Software Release 12.4> Release Notes> Cisco IOS Release 12.4

- *Cross-Platform Release Notes for Cisco IOS Release 12.4T*

  On Cisco.com at:

  Products and Services > Cisco IOS Software >Cisco IOS Release 12.4>General Information>Release Notes> Cross-Platform Release Notes

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software> Cisco IOS Software Release 12.4> Release Notes> Cisco IOS Release 12.4T

- Product bulletins, field notices, and other release-specific documents at http://www.cisco.com/univercd/home/index.htm

- *Caveats for Cisco IOS Release 12.4*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.4 XB" in these release notes, see *Caveats for Cisco IOS Release 12.4* which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.4 .

  On Cisco.com at:

  Products and Services > Cisco IOS Software >Cisco IOS Release 12.4>General Information>Release Notes>Cross-Platform Release Notes for Cisco IOS Release 12.4, Part 5: Caveats

On http://www.cisco.com/univercd/home/index.htm at:

Cisco IOS Software > Cisco IOS Software Release 12.4 > Release Notes > Cisco IOS Release 12.4>Cross-Platform Release Notes for Cisco IOS Release 12.4, Part 5: Caveats

- *Caveats for Cisco IOS Release 12.4T*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.4 XB" in these release notes, see *Caveats for Cisco IOS Release 12.4 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.4 T.

  On Cisco.com at:

  Products and Services > Cisco IOS Software >Cisco IOS Release 12.4>General Information>Release Notes>Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 5: Caveats

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software > Cisco IOS Release 12.4 > Release Notes> Cisco IOS Release 12.4> Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 5: Caveats

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 Mainline> Troubleshoot and Alerts > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may 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.)

Platform-Specific Documents

These documents are available for the Cisco 7200 series routers located on Cisco.com and http://www.cisco.com/univercd/home/index.htm:

Cisco 7200 VXR Installation and Configuration Guide

- *Cisco 7206 Installation and Configuration Guide*
- *Cisco 7204 Installation and Configuration Guide*
- *Quick Reference for Cisco 7204 Installation*
- *Cisco 7202 Installation and Configuration Guide*

On Cisco.com at:

Products & Services>Routers>Cisco 7200 Series Routers

On http://www.cisco.com/univercd/home/index.htm at:

Cisco Product Documentation: **All Product Documentation: Core/High-End Routers**

These documents are available for the Cisco 7100 series VPN routers located on Cisco.com and http://www.cisco.com/univercd/home/index.htm:

- *Quick Start Guide Cisco 7100 Series VPN Router*

On Cisco.com at:

Products & Services>End-of-Sale and End-of-Life Products>Security>Cisco 7100 Series VPN Routers

On http://www.cisco.com/univercd/home/index.htm at:

Cisco Product Documentation: **All Product Documentation: Core/High-End Routers**

These documents are available for the Cisco 7000 series routers located on Cisco.com and http://www.cisco.com/univercd/home/index.htm:

- *Cisco 7010 User Guide*
- *Cisco 7000 User Guide*
- *Cisco 7000 Hardware Installation and Maintenance*

On Cisco.com at:

Products & Services>End-of-Sale and End-of-Life Products>Cisco 7000 Series Routers

On http://www.cisco.com/univercd/home/index.htm at:

Cisco Product Documentation: **All Product Documentation: Core/High-End Routers**

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.4(2)XB and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Products and Services > Cisco IOS Software > Cisco IOS Release 12.4 > Configure> Feature Guides

On Cisco.com at:

Products and Services > Cisco IOS Software > Cisco IOS Release 12.4T > Configure> Feature Guides

On http://www.cisco.com/univercd/home/index.htm at:

Cisco IOS Software > Cisco IOS Release 12.4 > New Feature Documentation

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

http://www.cisco.com/go/fn

Open Source License Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT

NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments regarding Cisco IOS software release notes and caveats documentation to relnote-feedback@cisco.com.

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:
  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 37.