



Release Notes for Cisco 7000 Family for Cisco IOS Release 12.3 YQ

August 8, 2007

Cisco IOS Release 12.3(14)YQ8

OL-7519-09

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.3(14)YQ8. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(14)YQ8, see the [“Caveats for Cisco IOS Release 12.3 YQ” section on page 8](#) and *Caveats for Cisco IOS Release 12.3*. 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 12.3* located on Cisco.com and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 5](#)
- [MIBs, page 7](#)
- [Important Notes, page 7](#)
- [Caveats for Cisco IOS Release 12.3 YQ, page 8](#)
- [Related Documentation, page 26](#)
- [Obtaining Documentation, page 32](#)
- [Obtaining Technical Assistance, page 33](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(14)YQ8 and includes the following sections:

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 2](#)
- [Determining the Software Version, page 2](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Support, page 3](#)

Memory Recommendations

Table 1 *Memory Recommendations for the Cisco IOS Release 12.3(14)YQ*

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

Supported Hardware

Cisco IOS Release 12.3(14)YQ8 supports the following Cisco 7000 platforms:

- Cisco 7200 series routers

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 12.3(14)YQ8:

```
Router> show version
Cisco IOS Software, 7301 Software (c7200-g8ik8s-mz), Version 12.3(14)YQ7, RELEASE
SOFTWARE (fc1)
```

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

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS and Catalyst OS 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.

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

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

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 12.3 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://www.cisco.com/register>

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

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 12.3 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 **12.3**.
 - 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 12.3, 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 **12.3** 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 12.3 YQ:

New Hardware Features in Cisco IOS Release 12.3(14)YQ8

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ8.

New Software Features in Cisco IOS Release 12.3(14)YQ8

There are no new software features supported in Cisco IOS Release 12.3(14)YQ8.

New Hardware Features in Cisco IOS Release 12.3(14)YQ7

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ7.

New Software Features in Cisco IOS Release 12.3(14)YQ7

There are no new software features supported in Cisco IOS Release 12.3(14)YQ7.

New Hardware Features in Cisco IOS Release 12.3(14)YQ6

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ6.

New Software Features in Cisco IOS Release 12.3(14)YQ6

There are no new software features supported in Cisco IOS Release 12.3(14)YQ6.

New Hardware Features in Cisco IOS Release 12.3(14)YQ5

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ5.

New Software Features in Cisco IOS Release 12.3(14)YQ5

There are no new software features supported in Cisco IOS Release 12.3(14)YQ5.

New Hardware Features in Cisco IOS Release 12.3(14)YQ4

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ4.

New Software Features in Cisco IOS Release 12.3(14)YQ4

There are no new software features supported in Cisco IOS Release 12.3(14)YQ4.

New Hardware Features in Cisco IOS Release 12.3(14)YQ3

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ3.

New Software Features in Cisco IOS Release 12.3(14)YQ3

There are no new software features supported in Cisco IOS Release 12.3(14)YQ3.

New Hardware Features in Cisco IOS Release 12.3(14)YQ2

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ2.

New Software Features in Cisco IOS Release 12.3(14)YQ2

There are no new software features supported in Cisco IOS Release 12.3(14)YQ2.

New Hardware Features in Cisco IOS Release 12.3(14)YQ1

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ1.

New Software Features in Cisco IOS Release 12.3(14)YQ1

There are no new software features supported in Cisco IOS Release 12.3(14)YQ1.

New Hardware Features in Cisco IOS Release 12.3(14)YQ

There are no new hardware features supported in Cisco IOS Release 12.3(14)YQ.

New Software Features in Cisco IOS Release 12.3(14)YQ

There are no new software features supported in Cisco IOS Release 12.3(14)YQ.

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

The following sections contain important notes about Cisco IOS Release 12.3(14)YQ5 that can apply to the Cisco 7000 family.

Deferrals

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

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

Field Notices and Bulletins

For general information about the types of documents listed in this section, refer to the following document:

http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/1654_pp.htm

- **Field Notices**—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- **Product Bulletins**—If you have an account on Cisco.com, you can find product bulletins at <http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml>. If you do not have a Cisco.com login account, you can find product bulletins at <http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml>.
- **What's Hot in Software Center**—*What's Hot in Software Center* provides information about caveats that are related to deferred software images. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases* at <http://www.cisco.com/kobayashi/sw-center> or by logging in and selecting **Technical Support > Software Center > Cisco IOS Software > What's Hot in Software Center**.
- **What's New for IOS** — *What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml> or by logging into Cisco.com and selecting **Technical Support > Software Center > Products and Downloads > Cisco IOS Software**.

Caveats for Cisco IOS Release 12.3 YQ

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 12.3 and Cisco IOS Release 12.3 T are also in Cisco IOS Release 12.3(14)YQ8.

For information on caveats in Cisco IOS Release 12.3, see *Caveats for Cisco IOS Release 12.3*.

For information on caveats in Cisco IOS Release 12.3 T, see *Caveats for Cisco IOS Release 12.3 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 with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, **log in** to Cisco.com and click **Service and Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

Table 2 Caveats Reference for Cisco IOS Release 12.3 YQ

DDTS Number	Open in Release	Resolved in Release
CSCee78300		12.3(14)YQ4
CSCef29307	12.3(14)YQ, 12.3(14)YQ1, 12.3(14)YQ2	12.3(14)YQ3
CSCef32820		12.3(14)YQ
CSCef60659		12.3(14)YQ
CSCef85449		12.3(14)YQ
CSCeg03019	12.3(14)YQ2, 12.3(14)YQ3, 12.3(14)YQ5, 12.3(14)YQ6, 12.3(14)YQ7, 12.3(14)YQ8	
CSCeg14007		12.3(14)YQ
CSCeg48467		12.3(14)YQ
CSCeg59866		12.3(14)YQ
CSCeg59994		12.3(14)YQ
CSCeg75992		12.3(14)YQ
CSCeg76716		12.3(14)YQ
CSCeh56402		12.3(14)YQ7
CSCeh69873		12.3(14)YQ4
CSCei37916	12.3(14)YQ2, 12.3(14)YQ3, 12.3(14)YQ4	
CSCei61732		12.3(14)YQ3
CSCei87444	12.3(14)YQ5, 12.3(14)YQ6, 12.3(14)YQ7, 12.3(14)YQ8	
CSCej48454		12.3(14)YQ4
CSCej79360		12.3(14)YQ4
CSCek26492		12.3(14)YQ8
CSCek37177		12.3(14)YQ8
CSCin73156		12.3(14)YQ3
CSCin98692	12.3(14)YQ5	12.3(14)YQ6
CSCin99850		12.3(14)YQ8
CSCsa52807		12.3(14)YQ
CSCsa53334		12.3(14)YQ8
CSCsa59334		12.3(14)YQ

Table 2 Caveats Reference for Cisco IOS Release 12.3 YQ (continued)

CSCsa59600		12.3(14)YQ
CSCsa61864		12.3(14)YQ
CSCsa62111		12.3(14)YQ
CSCsa71768	12.3(14)YQ1	12.3(14)YQ2
CSCsa81130	12.3(14)YQ1	12.3(14)YQ2
CSCsa88059	12.3(14)YQ1	12.3(14)YQ2
CSCsb06658		12.3(14)YQ8
CSCsb11124		12.3(14)YQ4
CSCsb14725	12.3(14)YQ2	
CSCsb24007		12.3(14)YQ2
CSCsb28691	12.3(14)YQ3	12.3(14)YQ4
CSCsb33035	12.3(14)YQ2	
CSCsb39865		12.3(14)YQ3
CSCsb84438		12.3(14)YQ4
CSCsc05462		12.3(14)YQ4
CSCsc11366	12.3(14)YQ5, 12.3(14)YQ6	
CSCsc12583	12.3(14)YQ5, 12.3(14)YQ6	
CSCsc31776		12.3(14)YQ4
CSCsd66755		12.3(14)YQ6
CSCsd80775		12.3(14)YQ6
CSCse62599		12.3(14)YQ8
CSCse64581		12.3(14)YQ8

Open Caveats—Cisco IOS Release 12.3(14)YQ8

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ8 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg03019

CEF may not work over different tunnels.

This issue occurs when both GRE and IPsec tunnels are configured, and the packet traverses both.

There are no known workarounds.

- CSCei87444

A Cisco Gateway GPRS Serving Node (GGSN) with an encrypted image may reload when having a heavy load.

This issue occurs only when the CPU is consistently over 96% for a long timeframe and 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.

Resolved Caveats—Cisco IOS Release 12.3(14)YQ8

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ8. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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>

- CSCek37177

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

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

This issue is documented as Cisco bug ID [CSCek37177](#).

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-20070124-crafted-tcp.shtml>

- CSCin99850

A Cisco Gateway GPRS Serving Node (GGSN) crashes while executing the **show gprs gtp pdp tid** command.

This issue occurs during multiple PDP creates and deletes.

Workaround: Avoid using the **show gprs gtp pdp tid** command.

- CSCsa53334

The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

- Fragmented IP packets may be used to evade signature inspection.
- IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at:

<http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml>.

- CSCsb06658

A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.

Cisco is making free software available to address this vulnerability for affected customers. 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-20060920-docsis.shtml>.

- CSCse62599

A Cisco Gateway GPRS Serving Node (GGSN) reloads when certain rare passwords are used.

This issue occurs only when the create request is using the Virtual Access Point Name (APN) feature and the password contains the “@” character.

Workaround: Do not use the Virtual APN feature to get the real APN name if the username contains the “@” character; instead use the pre-authenticate Virtual APN feature.

- CSCse64581

A Cisco Gateway GPRS Serving Node (GGSN) running the R5.x/R6.0 image reloads when a secondary create PDP context request includes a traffic flow template (TFT) information element (IE) that contains the TFT code "No TFT operation" and the packet has a filter in it.

This issue occurs only when debug gprs gtp parsing is enabled.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YQ7

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ7 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg03019

CEF may not work over different tunnels.

This issue occurs when both GRE and IPsec tunnels are configured, and the packet traverses both.

There are no known workarounds.

- CSCei87444

A Cisco Gateway GPRS Serving Node (GGSN) with an encrypted image may reload when having a heavy load.

This issue occurs only when the CPU is consistently over 96% for a long timeframe and 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.

Resolved Caveats—Cisco IOS Release 12.3(14)YQ7

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ7. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeh56402

A router may crash when you shut down the Frame Relay interface of a peer.

This issue occurs only on a Cisco router that connects to the peer using a serial interface that has Frame Relay encapsulation and encryption enabled.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YQ6

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ6 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg03019

CEF may not work over different tunnels.

This issue occurs when both GRE and IPIP tunnels are configured, and the packet traverses both.

There are no known workarounds.

- CSCei87444

A Cisco Gateway GPRS Serving Node (GGSN) with an encrypted image may reload when having a heavy load.

This issue occurs only when the CPU is consistently over 96% for a long timeframe and 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.

- CSCsc11366

A MWAM Processor running IOS Release 12.3(14)YQ2 may experience an input queue high problem. If the input queue is kept in high level for a long time, new input packets may be dropped. If the image is without the CSCej48454 fix, input queue wedge could occur after arp entries are aged.

This issue occurs under the following conditions:

- The charging path is TCP and the charging gateway sends a node-alive msg.
- A large number of CDRs pile up in GGSN and needs to be sent to the charging gateway.
- The “redirect all” feature needs to be enable in APN, and a large number of MS packet can not be cef switch and needs to enqueue for slow process (maybe has option field in the IP header).

The root cause of this issue is that the process is blocked in TCP write and can not take care of the queued data packets in a timely fashion. These packets pile up in the input queue and block new input packets.

Workaround: Load an image with the CSCej48454 fix (Cisco IOS Release 12.3(14)YQ4 or later).

Resolved Caveats—Cisco IOS Release 12.3(14)YQ6

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCin98692

A Cisco Gateway GPRS Serving Node (GGSN) may reload when executing the **show aaa attribute protocol radius** command.

This issue only occurs if the **show aaa attribute protocol radius** command is executed from the Command Line Interface.

There are no known workarounds.

- CSCsc12583

A Cisco Gateway GPRS Serving Node (GGSN) may reload under control and data traffic stress conditions.

This issue occurs when consecutive actions of create and delete requests for a large number PDP Contexts occur at a very high rate, especially when not enough time is allowed for all the contexts to be established or cleaned up properly.

There are no known workarounds.

- CSCsd66755

In Cisco GGSN, when Interim Accounting is not configured, the updated values of SGSN address and QOS Negotiated do not appear in the Accounting-Stop message.

This issue occurs under the following conditions:

- Interim accounting is not configured under the APN.
- A GTPv1 PDP is created.
- An Update request is received with a new SGSN Address or QOS Negotiated value.
- The PDP is deleted.
- 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

A Cisco Gateway GPRS Serving Node (GGSN) is sending a wrong Message-length value for 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 issue occurs when setting a message in the Message Field of PPP PAP. This does not have an operational impact as PAP authentication passes successfully, but it causes monitoring issues.

Workaround: Configure the command `gprs gtp response-message pcp ipcp message-length` at global scope. This will cause the message length subfield to be included in the PAP Authenticate-Acl frame.

Open Caveats—Cisco IOS Release 12.3(14)YQ5

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg03019

CEF may not work over different tunnels.

This issue occurs when both GRE and IPIP tunnels are configured, and the packet traverses both.

There are no known workarounds.

- CSCei87444

A Cisco Gateway GPRS Serving Node (GGSN) with an encrypted image may reload when having a heavy load.

This issue occurs only when the CPU is consistently over 96% for a long timeframe and 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.

- CSCin98692

A Cisco Gateway GPRS Serving Node (GGSN) may reload when executing the **show aaa attribute protocol radius** command.

This issue occurs only if the **show aaa attribute protocol radius** command is executed from the Command Line Interface.

There are no known workarounds.

- CSCsc11366

A MWAM Processor running IOS Release 12.3(14)YQ2 may experience an input queue high problem. If the input queue is kept in high level for a long time, new input packets may be dropped. If the image is without the CSCej48454 fix, input queue wedge could occur after arp entries are aged.

This issue occurs under the following conditions:

- The charging path is TCP and the charging gateway sends a node-alive msg.
- A large number of CDRs pile up in GGSN and needs to be sent to the charging gateway.
- The “redirect all” feature needs to be enable in APN, and a large number of MS packet can not be cef switch and needs to enqueue for slow process (maybe has option field in the IP header).

The root cause of this issue is that the process is blocked in TCP write and can not take care of the queued data packets in a timely fashion. These packets pile up in the input queue and block new input packets.

Workaround: Load an image with the CSCej48454 fix (Cisco IOS Release 12.3(14)YQ4 or later).

- CSCsc12583

A Cisco Gateway GPRS Serving Node (GGSN) may reload under control and data traffic stress conditions.

This issue occurs when consecutive actions of create and delete requests for a large number PDP Contexts occur at a very high rate, especially when not enough time is allowed for all the contexts to be established or cleaned up properly.

There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(14)YQ5

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.3(14)YQ5.

Open Caveats—Cisco IOS Release 12.3(14)YQ4

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei37916

A Cisco Gateway GPRS Serving Node (GGSN) does not function properly when wait-accounting and AAA Broadcast Accounting are configured on an APN. When the first RADIUS server responds to an Accounting Start message, the GGSN establishes the PDP context without waiting for responses from all other RADIUS servers. Under a stress condition, the GGSN may reload.

This issue occurs on a Cisco platform that runs Cisco IOS Release 12.4 and GGSN Release 5.2 and occurs only when both wait-accounting and AAA Broadcast Accounting are configured together on an APN.

There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(14)YQ4

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCee78300

An unexpected bus error reload (that is, an illegal access to a low address) may occur in the RADIUS process.

This issue occurs on a Cisco 7200 series that is configured with an NPE-G1 and that runs Cisco IOS Release 12.3(9). However, this issue does not occur in Release 12.3(3).

There are no known workarounds.

- CSCeh69873

When the GGSN receives a PDP context with non-real time traffic classes and the SSD value is not 1 (that is, speech), the PDP is rejected.

This issue occurs as a result of not being CR-830 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.

- CSCej48454

The GGSN interface inputq may lose communication

This issue occurs under the following conditions:

- The APN redirect all feature needs to be enable.
- The GGSN receives a user payload packet addressed to the internal loopback address (127.0.0.x).
- The packet size is less than 1500.
- The packet needs to include something that can not be cef switched (i.e. ip option)

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

- CSCej79360

The TCP path between the charging gateway and Cisco GGSN flapping may drop some packets under the following conditions:

- Redirect all is enable in GGSN.
- many redirect all traffic need to punt to process level because there is ip option field in the packet.
- charging path is TCP.

This issue occurs because while the GGSN can send 128 charging msg simultaneously, the TCP send window is only 20K bytes; so many of the packet are dropped before getting out of GGSN. After max retry and no response, GGSN will mark the charging gateway down.

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

- CSCsb11124

The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

Cisco has published a Security Advisory on this issue; it is available at <http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

- CSCsb28691

A Cisco Gateway GPRS Serving Node (GGSN) that functions under stress may reload unexpectedly.

This issue occurs when the call rate is high (200 calls per second), when there are two Dynamic Host Configuration Protocol (DHCP) servers that respond very slowly, and when the GGSN is configured for session redundancy.

There are no known workarounds.

- CSCsb84438

A Cisco Gateway GPRS Serving Node (GGSN) may unexpectedly reload if the following condition persists for a long time:

- The Dynamic Host Configuration Protocol (DHCP) server is very slow.
- The user session activation is high.
- The DHCP lease is very short.

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

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

- CSCsc05462

In Cisco IOS Release 12.3(14)YQ3 (Cisco GGSN Release 5.2), a PLMN and QoS change at the same time will cause a duplicated volume report. The same byte counts are reported in successive containers, one added due record closure due to PLMN change, and the other due to QoS Change.

No charging profile was configured under the APN because it is not service-aware (GGSN functionality testing). SGSN did not send any Charging-characteristics value.

Workaround: Use an APN specific charging profile.

- CSCsc31776

In Cisco IOS GGSN Release 5.0 and 6.0, the router reloads when 3000 create requests are sent under the following conditions:

- The **debug gprs gtp message** is turned on.
- An external DHCP IP address assignment is configured.
- VRF is configured on the APN but not on the DHCP server.

After about 3000 create requests, the router unexpectedly reloads.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YQ3

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg03019

CEF may not work over different tunnels.

This issue occurs when both GRE and IP/IP tunnels are configured, and the packet traverses both.

There are no known workarounds.

- CSCei37916

A Cisco Gateway GPRS Serving Node (GGSN) running R5.2 shows incorrect behavior when wait-accounting is configured in an APN along with AAA broadcast accounting. When the first Radius server responds to Accounting Start, GGSN establishes the PDP context without waiting for responses from all other Radius servers. Sometimes under stress conditions, GGSN may reload.

This issue occurs only when both wait-accounting and AAA broadcast accounting are used together for an APN.

There are no known workarounds.

- CSCsb28691

A Cisco Gateway GPRS Serving Node (GGSN) that functions under stress may reload unexpectedly. This issue occurs when the call rate is high (200 calls per second), when there are two DHCP servers that respond very slowly, and when the GGSN is configured for session redundancy.

There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(14)YQ3

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef29307

Cisco GGSN does not clear the TCP socket from the GGSN to the charging gateway. This makes the GGSN unresponsive to Nodealive requests from the charging gateway if the Charging Functionality is under a lot stress, and the charging gateway is going up and down frequently, resulting in a lot of charging data records being queued.

Workaround: Execute the **show tcp brief** command to display the tcb value. Then enter the **clear tcp tcb** command to clear the tcb using the tcb value from the **show tcp brief command** command. Then send Nodealive from the charging gateway.

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

- CSCin73156

Cisco GGSN does not negotiate the Qos values properly when an wrong Qos profile of all 0's is sent in as a request in the R98 format.

There are no known workarounds.

- CSCsb39865

In a Cisco Gateway GPRS Support Node (GGSN) running release 5.2 and 6.0 software, the CAUSE IE in PDP update-context-response from GGSN shall be set to 201 (Mandatory IE incorrect) upon receiving a PDP update-context-request with Max Bit-Rate (MBR) set to 0 KBPS.

This occurs when SGSN sends PDP update-context-request to GGSN with Uplink/Downlink Max Bit Rate (MBR) set to zero KBPS.

There are no known workarounds.

Open Caveats—Cisco IOS Release 12.3(14)YQ2

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef29307

Cisco GGSN does not clear the TCP socket from the GGSN to the charging gateway. This makes the GGSN unresponsive to Nodealive requests from the charging gateway if the Charging Functionality is under a lot of stress, and the charging gateway is going up and down frequently, resulting in a lot of charging data records being queued.

Workaround: Execute the **show tcp brief** command to display the tcb value. Then enter the **clear tcp tcb** command to clear the tcb using the tcb value from the **show tcp brief** command. Then send Nodealive from the charging gateway.

- CSCeg03019

CEF may not work over different tunnels.

This issue occurs when both GRE and IP/IP tunnels are configured, and the packet traverses both.

There are no known workarounds.

- CSCei37916

A Cisco GGSN running R5.2 shows incorrect behavior when wait-accounting is configured in an APN along with AAA broadcast accounting. When the first Radius server responds to Accounting Start, GGSN establishes the PDP context without waiting for responses from all other Radius servers. Sometimes under stress conditions, GGSN may reload.

This issue occurs only when both wait-accounting and AAA broadcast accounting are used together for an APN.

There are no known workarounds.

- CSCsb14725

The `cgprsCgProfileVolumeLimit` object accepts invalid values from SNMP.

This issue occurs when the value for `cgprsCgProfileVolumeLimit` is written using the **setany** command.

There are no known workarounds.

- CSCsb24007

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>

- CSCsb33035

The Gateway GPRS support node (GGSN) may cause some packet looping with two GRE headers.

This issue is observed under the following conditions:

- GGSN down stream traffic comes in from VRF GRE tunnel.
- Cef switch is enable but the cef switch fails for some reason similar to ACL failure or no user identified to receive the packet.
- There are two default routes in the VRF routing table to route traffic back to the same direction.

Workaround: Turn off cef or not use VRF. However, this is not recommended.

Resolved Caveats—Cisco IOS Release 12.3(14)YQ2

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsa71768

Charging characteristics selection mode is set to roaming default for a roaming user when there is no default profile on GGSN.

This issue occurs when there is no default profile in GGSN.

There are no known workarounds.

- CSCsa81130

Radius accounting request packet from GGSN to Radius does not have CLASS attribute.

This issue occurs in pdp type PPP for both gtp v0 and gp v1.

There are no known workarounds.

- CSCsa88059

Adding a secondary/tertiary gateway does not work.

This issue occurs only when non default port is used for gprs charging.

Workaround: Unconfigure all CGs followed by configure all the CGs.

Open Caveats—Cisco IOS Release 12.3(14)YQ1

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef29307

Cisco GGSN does not clear the TCP socket from the GGSN to the charging gateway and hence does not respond to the Nodealive requests from the charging gateway, under the condition that the Charging Functionality is under a lot stress and the charging gateway is going up and down frequently resulting in a lot of charging data records being queued.

Workaround: Execute the **show tcp brief** command to display the tcb value. Then enter the **clear tcp tcb** command to clear the tcb using the tcb value from the **show tcp brief command** command. Then send Nodealive from the charging gateway.

- CSCsa71768
Charging characteristics selection mode is set to roaming default for a roaming user when there is no default profile on GGSN.
This issue occurs when there is no default profile in GGSN.
There are no known workarounds.
- CSCsa81130
Radius accounting request packet from GGSN to Radius does not have CLASS attribute.
This issue occurs in pdp type PPP for both gtp v0 and gp v1.
There are no known workarounds.
- CSCsa88059
Adding a secondary/tertiary gateway does not work.
This issue occurs only when non default port is used for gprs charging.
Workaround: Unconfigure all CGs followed by configure all the CGs.

Resolved Caveats—Cisco IOS Release 12.3(14)YQ1

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.3(14)YQ1.

Open Caveats—Cisco IOS Release 12.3(14)YQ

This section documents possible unexpected behavior by Cisco IOS Release 12.3(14)YQ and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef29307
Cisco GGSN does not clear the TCP socket from the GGSN to the charging gateway and hence does not respond to the Nodealive requests from the charging gateway, under the condition that the Charging Functionality is under a lot stress and the charging gateway is going up and down frequently resulting in a lot of charging data records being queued.
Workaround: Execute the **show tcp brief** command to display the tcb value. Then enter the **clear tcp tcb** command to clear the tcb using the tcb value from the **show tcp brief command** command. Then send Nodealive from the charging gateway.

Resolved Caveats—Cisco IOS Release 12.3(14)YQ

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef32820

Cisco GGSN Deletes and create the PDP context again under the condition that the new create request for an already existing context is coming for GTPv0 and that it is coming from a different SGSN than the earlier one and this new SGSN already is having a few active contexts with the same GGSN and the Restart count value in this new create request is different.

There are no known workarounds.

- CSCef60659

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>

- CSCef85449

GGSN will continue duration limit trigger for CDRs which belong to PDPs, which are in the process of deletion.

This issue occurs when the charging profile, which is selected by PDP, has duration limit in it and PDP context is in “to be deleted” state.

There are no known workarounds.

- CSCeg14007

When a PDP context of type PPP is established on the GGSN without the use of L2TP, the GGSN tries to set up a AAA authentication group list for this context, even when AAA new-model is not configured. This results in a failure in establishing this context with the following debug message printed out:

```
GTP-PPP: Fail to install aaa-group lists
```

This issue occurs on GGSN Release 5.0 when the involved APN for this PDP context is in non-transparent access-mode.

Workaround: Do not configure the aaa-group under the APN when AAA new-model is not used.

- CSCeg48467

With very high rate of IP PDP signaling and very high rate of viable length packets over all open contexts for a long period of time, GGSN may show wrong “available BW” in the output of command **show gprs bandwidth status <>**.

There are no known workarounds.

- CSCeg59866

GGSN does spurious memory access while creating pdp context in maintenance-mode.

This issue occurs when GGSN is in maintenance mode.

There are no known workarounds.

- CSCeg59994

GGSN will not reject pdp update request. It will return cause value 128, and it will not increment the mandatory IE incorrect counter.

This issue occurs when SGSN sends an update request with incorrect length QOS.

There are no known workarounds.

- CSCeg75992

A Cisco router running gateway GPRS support node software (GGSN) does not send tunnel end-point identifier (TEID) control in the update response if TEID-C is previously confirmed by the SGSN.

This is not a problem. However, to help interoperation with SGSNs, which only talk GTPv0 with each other but can talk GTPv1 with GGSN, the new SGSN needs to know the TEID-C of the PDP context.

There are no known workarounds.

- CSCeg76716

After enough number of mobiles fail to establish contexts due to username errors, domain name errors, or internal memory allocation problems, the GGSN fails to accept any further Create Requests to establish such contexts. This is caused by the count for the max number of pending PPP-Regen contexts reaching the max without recovering back to zero, which is shown in the output of the command **show gprs gtp statistic** behind the entry “ppp_regen_pending”.

This issue occurs in Cisco GGSN of release R4.0 or later which has some APNs configured to use PPP-Regeneration to handle IP PDP contexts.

Workaround: Configure a larger max using the global config command **gprs gtp ppp-regeneration max-pending** command. However, this may introduce a consequence that when the activation rate of such PPP-Regen PDP contexts is high, high PPP and L2TP traffic will be resulted between the GGSN and other LNSes/PDNs.

- CSCsa52807

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>

- CSCsa59334

SYSLOG message returns NULL in the APN field.

This issue occurs when GTP authentication fails:

```
%GPRSFLTMG-4-GTPv1AAAFAIL_PDPACTIVATIONFAIL: GSN: <snip> APN: NULL, <snip>
```

There are no known workarounds.

- CSCsa59600

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>

- CSCsa61864

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.cpni.gov.uk/docs/re-20050412-00303.pdf>

- CSCsa62111

Packets may be stuck in the input queue of a Cisco 7200 series.

This issue occurs on a Cisco 7200 series running a Cisco IOS interim Release 12.3(12.10) and configured with an NPE-G1.

Workaround: Reload the router to clear the input queue or increase the input queue beyond the default limit of 75 via the **hold-queue** *length* command.

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 27](#)
- [Platform-Specific Documents, page 27](#)
- [Feature Modules, page 28](#)
- [Cisco IOS Software Documentation Set, page 28](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.3*

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

Technical Documents

- *Caveats for Cisco IOS Release 12.3(14)YQ*

As a supplement to the caveats listed in “[Caveats for Cisco IOS Release 12.3 YQ](#)” in these release notes, see *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Caveats

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Caveats



Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/bugtool.shtml>.

Platform-Specific Documents

These documents are available for the Cisco 7000 family of routers on Cisco.com and the Documentation CD-ROM:

- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7200 Routers Quick Start Guide*

On Cisco.com at:

Technical Documents: All Product Documentation: Core/High-End Routers

On the Documentation CD-ROM at:

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

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.3(14)YQ 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:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: 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>

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Configuration Guides and Command References

Cisco IOS Release 12.3 Documentation Set Contents

Table 3 lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.



Note

You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3

Table 3 *Cisco IOS Release 12.3 Documentation Set*

Books	Major Topics
<ul style="list-style-type: none"> <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	<ul style="list-style-type: none"> Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2</i> 	<ul style="list-style-type: none"> Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server

Table 3 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Technologies Configuration Guide: Dial Access</i> • <i>Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications</i> • <i>Cisco IOS Dial Technologies Command Reference, Volume 1 of 2</i> • <i>Cisco IOS Dial Technologies Command Reference, Volume 2 of 2</i> 	<ul style="list-style-type: none"> Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	<ul style="list-style-type: none"> LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP Configuration Guide</i> • <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> • <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> • <i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i> 	<ul style="list-style-type: none"> IP Addressing IP Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	<ul style="list-style-type: none"> AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	<ul style="list-style-type: none"> Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i> • <i>Cisco IOS Voice, Video, and Fax Command Reference</i> 	<ul style="list-style-type: none"> Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	<ul style="list-style-type: none"> Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 3 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i> 	General Packet Radio Service
<ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> 	ARA LAT NAS1 Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Error Messages</i> • <i>New Features in 12.3-Based Limited Lifetime Releases</i> • New Features in Release 12.3 T • Release Notes (Release note and caveat documentation for 12.3-based releases and various platforms) 	

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at

<http://www.cisco.com>.

Translated documentation can be accessed at

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco products documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section on page 26.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Copyright © 2007
Cisco Systems, Inc.
All rights reserved.

