Release Notes for Cisco AS5400 Universal Gateways for Cisco IOS Release 12.2(15)ZK5

August 18, 2004

Cisco IOS Release 12.2(15)ZK5

OL-4770-01 Rev. E1

These release notes for the Cisco AS5400 universal gateway describe the enhancements provided in Cisco IOS Release 12.2(15)ZK5. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(15)ZK4, see "Caveats for Cisco IOS Release 12.2(15)ZK" section on page 9. See also *Caveats for Cisco IOS Release 12.2*, which 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 12.2 T* for Cisco IOS Release 12.2(15)T9 located on Cisco.com and the Documentation CD-ROM.

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.

Contents

These release notes describe the following topics:

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

Inheritance Information

Cisco IOS Release 12.2(15)ZK5 is based on Cisco IOS Release 12.2(15)T9. All features in Cisco IOS Release 12.2(15)T9 are in Cisco IOS Release 12.2(15)ZK5.

Table 1 lists sections of the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* that apply to Cisco IOS Release 12.2(15)ZK5.

Table 1 References for the Cross-Platform Release Notes for Cisco IOS Release 12.2 T

Topic	Location
• Introductory information about the Cisco AS5400 universal gateway • Hardware Supported • Feature Set Tables • Additional Notes for the Cisco AS5400 Universal Gateways	On Cisco.com at: **Products & Services**: **IOS Software**: **Cisco IOS Software Releases 12.2 T**: **Instructions and Guides**: **Release Notes**: **Cross-Platform Release Notes for Cisco IOS Release 12.2 T, Part 2: Platform-Specific Information** Or at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tfeat.htm
• Determining the Software Version • Upgrading to a New Software Release	On Cisco.com at: **Products & Services**: **IOS Software**: **Cisco IOS Software Releases 12.2 T**: **Instructions and Guides**: **Release Notes**: **Cross-Platform Release Notes for Cisco IOS Release 12.2 T, Part 1: System Requirements** Or at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122treqs.htm
• Feature Descriptions (New and Changed Information) • MIBs • Important Notes	On Cisco.com at: **Products & Services**: **IOS Software**: **Cisco IOS Software Releases 12.2 T**: **Instructions and Guides**: **Release Notes**: **Cross-Platform Release Notes for Cisco IOS Release 12.2 T, Part 3: New Features and Important Notes** Or at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tnewf.htm

Table 1 References for the Cross-Platform Release Notes for Cisco IOS Release 12.2 T (continued)

Topic	Location
• Related Documentation • Obtaining Documentation • Obtaining Technical Assistance	On Cisco.com at: **Products & Services**: **IOS Software**: **Cisco IOS Software Releases 12.2 T**: **Instructions and Guides**: **Release Notes**: **Cross-Platform Release Notes for Cisco IOS Release 12.2 T, Part 4: Related Documentation** Or at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/122tdocs.htm

Introduction

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.2(15)ZK5, see the "New and Changed Information" section on page 7.

Early Deployment Releases

These release notes describe the Cisco AS5400 universal gateway for Cisco IOS Release 12.2(15)ZK5, which is an early deployment (ED) release based on Cisco IOS Release 12.2(15)T9. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features. Table 2 shows recent early deployment releases for the CiscoAS5400 universal gateway.

Table 2 Early Deployment Release New Features for the Cisco AS5400 Universal Gateway

ED Release	Maintenance Release	Additional Software Features	Additional Hardware Features	Availability
Cisco IOS Release 12.2(15)ZK5	12.2(15)ZK5	None	None	Now
Cisco IOS Release 12.2(15)ZK4	12.2(15)ZK4	None	None	Now
Cisco IOS Release 12.2(15)ZK3	12.2(15)ZK3	None	None	Now
Cisco IOS Release 12.2(15)ZK2	12.2(15)ZK2	None	None	Now
Cisco IOS Release 12.2(15)ZK1	12.2(15)ZK1	Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks	None	Now
Cisco IOS Release 12.2(15)ZK		Policy-Based Routing Attribute 104 and Policy-Based Route Map	None	Now

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(15)ZK5 and includes the following sections:

Memory Recommendations

Table 3 Memory Recommendations for the Cisco AS5400 Universal Gateways

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco AS5400	IP Standard Feature Set	IP Plus	c5400-is-mz	32 MB Flash	256 MB DRAM	RAM
		IP Plus IPsec 56	c5400-ik8s-mz	32 MB Flash	256 MB DRAM	RAM
	Enterprise Standard Feature Set	Enterprise Plus	c5400-js-mz	32 MB Flash	256 MB DRAM	RAM
		Enterprise Plus IPsec 56	c5400-jk8s-mz	32 MB Flash	256 MB DRAM	RAM
		Enterprise Plus IPsec 3DES	c5400-jk9s-mz	32 MB Flash	256 MB DRAM	RAM
Cisco AS5400HPX	IP Standard Feature Set	IP Plus	c5400-is-mz	32 MB Flash	256 MB DRAM	RAM
		IP Plus IPsec 56	c5400-ik8s-mz	32 MB Flash	256 MB DRAM	RAM
	Enterprise Standard Feature Set	Enterprise Plus	c5400-js-mz	32 MB Flash	256 MB DRAM	RAM
		Enterprise Plus IPsec 56	c5400-jk8s-mz	32 MB Flash	256 MB DRAM	RAM
		Enterprise Plus IPsec 3DES	c5400-jk9s-mz	32 MB Flash	256 MB DRAM	RAM

Supported Hardware

Cisco IOS Release 12.2(15)ZK5 supports the Cisco AS5400 universal gateway:

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 7.

For additional information about supported hardware for this platform and release, please refer to the Hardware/Software Compatibility Matrix in the Cisco Software Advisor at the following location:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Table 4 Supported Interfaces for the Cisco AS5400 Universal Gateway

Interface, Network Module, or Data Rate	Product Description	Supported Platforms
Dial/Voice Feature Cards [1]	AS54-DFC-CT3	All Cisco AS5400 universal gateway platforms
	AS54-DFC-60NP	All Cisco AS5400 universal gateway platforms
	AS54-DFC-108NP	All Cisco AS5400 universal gateway platforms
	2 PRI DFC, 4 PRI DFC, 8 PRI DFC	All Cisco AS5400 universal gateway platforms
LAN Interfaces	Fast Ethernet 10/100BaseT (RJ-45)	All Cisco AS5400 universal gateway platforms
Trunk/Backhaul Interface Options	2PRI CT1/CE1 DFC, 4PRI CT1/CE1 DFC, 8PRI CT1/CE1 DFC	All Cisco AS5400 universal gateway platforms
	CT3 DFC	All Cisco AS5400 universal gateway platforms
	2 serial ports on the motherboard	All Cisco AS5400 universal gateway platforms

1. The Voice/Fax network modules require Cisco IOS Plus feature sets.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco AS5400 universal gateway, log in to the Cisco AS5400 universal gateway and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 5400 Software (C5400-IS-MZ), Version 12.2(15)ZK4, EARLY DEPLOYMENT RELEASE
SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to *Software Installation and Upgrade Procedures* located at the following URL:

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

Feature Set Tables

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

Cisco IOS Release 12.2(15)ZK5 supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2(15)ZK5 can include new features supported by the Cisco AS5400 universal gateway.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 5 lists the features and feature sets supported by the Cisco AS5400 universal gateway in Cisco IOS Release 12.2(15)ZK5 and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, 12.2(15)ZK5 means a feature was introduced in 12.2(15)ZK5. If a cell in this column is empty, the feature was included in the initial base release.

Note The parent release for Cisco IOS Release 12.2(15)ZK5 is Cisco IOS Release 12.2(15)T. For information about inherited features, refer to Cisco.com or Cisco Feature Navigator. For Cisco.com, either go to Cisco.com and select the appropriate software release under **Products and Service** and **IOS Software** or go to http://www.cisco.com/univercd/home/index.htm and select the appropriate software release under **Cisco IOS Software** and **Release Notes**. If you have a Cisco.com login account, you can use the Cisco Feature Navigator tool at http://www.cisco.com/cgi-bin/Support/FeatureNav/FN.pl.

Table 5 Feature List by Feature Set for the Cisco AS5400 Universal Gateways

		Software Images by Feature Set				
Features	**In**	**IP Plus**	**IP Plus IPsec 56**	**Enterprise Plus**	**Enterprise Plus IPsec 56**	**Enterprise Plus**
Voice						
Policy-Based Routing	12.2(15)ZK	Yes	Yes	Yes	Yes	Yes
Attribute 104 and Policy-Based Route Map	12.2(15)ZK	Yes	Yes	Yes	Yes	Yes
Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks	12.2(15)ZK1	Yes	Yes	Yes	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco AS5400 universal gateway for Cisco IOS Release 12.2(15)ZK5.

New Hardware and Software Features in Cisco IOS Release 12.2(15)ZK2 to Cisco IOS Release 12.2(15)ZK5

No new hardware or software features are supported by the Cisco AS5400 universal gateway for Cisco IOS Release 12.2(15)ZK2 to Cisco IOS Release 12.2(15)ZK5.

New Hardware Features in Cisco IOS Release 12.2(15)ZK1

No new hardware features are supported by the Cisco AS5400 universal gateway for Cisco IOS Release 12.2(15)ZK1.

New Software Features in Cisco IOS Release 12.2(15)ZK1

The following new software feature is supported by the Cisco AS5400 universal gateway for Cisco IOS Release 12.2(15)ZK1:

Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks

The B-Channel ID features enables call management applications to identify the specific ISDN B-channel used during a voice gateway call to enable port specific features, such as voice recording and call transfer.

New Hardware Features in Cisco IOS Release 12.2(15)ZK

No new hardware features are supported by the Cisco AS5400 universal gateway for Cisco IOS Release 12.2(15)ZK.

New Software Features in Cisco IOS Release 12.2(15)ZK

The following new software features are supported by the Cisco AS5400 universal gateway for Cisco IOS Release 12.2(15)ZK:

Attribute 104 and Policy-Based Route Map

Attribute 104 and Policy-Based Route Map provides Permit Route Map, Default Private Route, Local PBR, and Pseudo Next-Hop Address.

Policy-Based Routing

Policy-Based routing (PBR) provides a mechanism for expressing and implementing forwarding and routing of data packets based on defined policies. The policies are based on decisions independent of the destination address such as the type of service, source address, precedence, port numbers, and protocol type.

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

Limitations and Restrictions

Attribute 104 increases the processing load on the route switch controller (RSC). Cisco IOS Release 12.2(15)ZK4 supports 40 percent of the maximum published total number of calls when running Attribute 104. Each Attribute 104 call can have up to 25 private routes.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(15)ZK4 that can apply to the Cisco AS5400 universal gateway.

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 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 12.2(15)ZK

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 open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.2 and Cisco IOS Release 12.2 T that apply to the Cisco AS5400 universal gateway are also in Cisco IOS Release 12.2(15)ZK4.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*.

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 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**: **Troubleshooting**: **Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Open Caveats—Cisco IOS Release 12.2(15)ZK5

There are no open caveats specific to Cisco IOS Release 12.2(15)ZK5 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.2(15)ZK5

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZK5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 6 Resolved Caveats for Cisco IOS Release 12.2(15)ZK5

DDTS ID Number	Description
CSCdz42788	Symptoms: When you make ISDN configuration changes on a Cisco 7204VXR router, bus errors may occur. Conditions: This symptom is observed on a Cisco 7204VXR router that is running Cisco IOS Release 12.2(12a). Workaround: There is no workaround.
CSCdz67303	Symptoms: A Cisco router that functions as a voice gateway may reload unexpectedly after a series of calls that include call transfers and diverted calls have been processed. Conditions: This symptom is observed on a Cisco 2621XM and Cisco 3640 when you use a third-party vendor protocol convertor to translate and provide a tunnel for Digital Private Network Signaling System (DPNSS) traffic over Q Signaling (QSIG). The symptom is not platform specific. Workaround: There is no workaround.
CSCea09674	Symptoms: All calls are dropped immediately when the **busyout** *slot* EXEC command is issued on a channelized T3 (CT3) dial feature card (DFC). Conditions: This symptom is observed on a Cisco AS5400 router that has a CT3 DFC in use and that has active dial modem calls. Workaround: Use the **busyout** *slot* EXEC command on all NextPort (NP 108)DFCs, the **busyout** *port* EXEC command, the Software Port Entity (SPE) **busyout** EXEC commands, or other **busyout** EXEC commands to clear calls gracefully without using the **busyout** *slot* EXEC command where the CT3 DFC is located.
CSCea25697	Symptoms: About 100 KB to 1 MB of processor memory may be lost when the **default interface** global configuration command is entered on a router. The memory loss can be detected by comparing the output of the **show memory** EXEC command by entering the **show memory** EXEC command both before and after configuring the **default interface** global configuration command on the router. Conditions: This symptom occurs only if the **default interface** global configuration command is configured on a router. Workaround: The memory loss can be avoided by manually unconfiguring interfaces using the **no** form of the interface configuration commands.
CSCea48995	Symptom: The information element (IE) of a calling party number in an outgoing call setup message may be corrupted. When you use the Q.931 Translator, the log files may display that the calling party number in the outgoing call setup message is "0x00," as in the following example: `ISDN Se0:23: TX -> SETUP pd = 8 callref = 0x0005 Bearer Capability i = 0x8890 Channel ID i = 0xA98397 Calling Party Number i = 0x00, (null), Plan:Unknown, Type:Unknown Calling Party SubAddr i = 0x80, '9876' Called Party Number i = 0x80, '2222', Plan:Unknown, Type:Unknown` Condition: This symptom is observed after an IE for a calling party subaddress is received. Workaround: There is no workaround.

Table 6 Resolved Caveats for Cisco IOS Release 12.2(15)ZK5 (continued)

DDTS ID Number	Description
CSCeb53422	Symptoms: A call setup failure may occur for high-delay links with a round-trip time greater than 300 milliseconds. Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2(16) but may also occur in other releases. The call fallback subsystem hard-codes the amount of time it will wait for the response to probes to 300 milliseconds. The probes fail if the round-trip time is more than 300 milliseconds, even though the network is a high-bandwidth network. Workaround: There is no workaround.
CSCeb85136	Symptoms: An IP packet that is sent with an invalid IP checksum may not be dropped. Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value. For example, in the situation where the IP checksum must be 0x1134 with a TTL of 3, if the packet is sent with an IP checksum of 0x1234 that is calculated by using a TTL value of 2, the packet is not dropped. In all other cases, packets with incorrect checksums are dropped. Workaround: There is no workaround.
CSCef29090	Symptoms: TCPClear sessions on a Cisco AS5850 may have throughput issues and slow response time. Conditions: This symptom was observed on a Cisco AS5850 with TCPclear sessions. Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(15)ZK4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)ZK4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 7 Open Caveats for Cisco IOS Release 12.2(15)ZK4

DDTS ID Number	Description
CSCea09674	Busyout (slot) with CT3 DFC drops all calls Symptoms: All calls are dropped immediately when the **busyout** *slot* EXEC command is issued on a channelized T3 (CT3) dial feature card (DFC). Conditions: This symptom is observed on a Cisco AS5400 router that has a CT3 DFC in use and that has active dial modem calls. Workaround: Use the **busyout** *slot* EXEC command on all NextPort (NP 108)DFCs, the **busyout** *port* EXEC command, the Software Port Entity (SPE) **busyout** EXEC commands, or other **busyout** EXEC commands to clear calls gracefully without using the **busyout** *slot* EXEC command where the CT3 DFC is located.

Table 7 Open Caveats for Cisco IOS Release 12.2(15)ZK4

DDTS ID Number	Description
CSCec80714	on AS5400 : cas call failed when for RPM service defined Symptoms: An incoming call may be rejected when the service that is defined in the *name* argument of the **resource-pool profile service** *name* global configuration command is applied to the customer profile. Conditions: This symptom is observed on a Cisco AS5300 and a Cisco AS5400 that are configured for R2 channel-associated signaling (CAS). Workaround: Remove the service from the **resource-pool profile service** *name* global configuration command.

Resolved Caveats—Cisco IOS Release 12.2(15)ZK4

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZK4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 Resolved Caveats for Cisco IOS Release 12.2(15)ZK4

DDTS ID Number	Description
CSCdu53656	A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem. Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.
CSCea28131	A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem. Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.
CSCed09146	Unwanted Extra STOP record seen for calls failing on authentication Symptoms: Extra network Accounting STOP record may be seen when an async call fails on authentication. These are unwanted records and should not be generated. Conditions: Seen for an Async call on 5300-T1 platform running 12.3(5.8) This problem was seen quite often and its may not be completely reproducible at will. This could be service affecting . Workaround: there is no workaround at this time.

Table 8 Resolved Caveats for Cisco IOS Release 12.2(15)ZK4 (continued)

DDTS ID Number	Description
CSCed27956	TCP checks should verify ack sequence number A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.
CSCed38527	TCP checks should verify ack sequence number A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability. This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software. A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Open Caveats—Cisco IOS Release 12.2(15)ZK3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)ZK3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 9 Open Caveats for Cisco IOS Release 12.2(15)ZK3

DDTS ID Number	Description
CSCec79011	<Word> option not available on the sh route-map dynamic ? command Symptoms: When using **sh route-map dynamic ?** the **Word** and <cr> options are missing on the Cisco AS5850 gateway. The command works but the options mentioned are missing from the help selections. Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(15)ZK3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZK3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 10 Resolved Caveats for Cisco IOS Release 12.2(15)ZK3

DDTS ID Number	Description
CSCdy33273	count from numbered ext ACL alone is punted from LC to RP Symptoms: Number of match count is punted up only for the extended numbered ACL. Workaround: There is no workaround.
CSCea53600	authorization failure for terminal login call with per-user DNS/WINS Symptoms: Authorization may fail for a terminal server login call. Conditions: This symptom is observed on a Cisco AS5400 when authorization occurs through a RADIUS-assigned Domain Name System (DNS) server or Microsoft Windows Internet Naming Service (WINS) server. Workaround: There is no workaround.
CSCeb27716	Spurious memory access at vp_fastsend() during stress Symptoms: Spurious memory access at vp_fastsend() may be seen in a Cisco AS5800 access server under stress. This may not be service affecting. Conditions: This is seen during stress test of 12 hours with bi-directional traffic setup. Workaround: There is no workaround.
CSCec59717	virtual profiles with PPP hangs in loop Symptoms: Terminal window PPP negotiation is failing intermittently on the Cisco AS5400. This issue is seen with async and V.120 digital calls. The client is a personal computer using the Microsoft Windows XP operating system. Workaround: There is no workaround.
CSCec64675	Need improvement to scale 5400 to 50 routes per user Symptoms: High CPU usage is observed on the Cisco AS5400 gateway when running with more than 25 routes per user using Attribute 104. Workaround: There is no workaround.

Table 10 Resolved Caveats for Cisco IOS Release 12.2(15)ZK3 (continued)

DDTS ID Number	Description
CSCec66146	Crash bus error at auth_tx_failure Symptoms: After some duration, the Network Access Server (NAS) will crash running Microsoft Challenge Authentication Protocol (MSCHAP) or MSCHAP V2. It is not certain if this may be timing influenced by async calls or something specific to the Cisco AS5400 gateway. Workaround: There is no work around.
CSCec78261	idle timer on tty not reset for terminal login async call Symptoms: On a Cisco AS5850 gateway, the idle timer on the TTY interface is not reset for interesting traffic for a terminal login async call. Workaround: There is no workaround.
CSCed02072	Memory leak in process CEF IPC Background on FBs Feature Board memory was not freed when the calls are disconnected. Symptoms: After running stress scenario on the Cisco AS5850 gateway for some duration, high CPU usage is observed on the feature board (FB). Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(15)ZK2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)ZK2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 11 Open Caveats for Cisco IOS Release 12.2(15)ZK2

DDTS ID Number	Description
CSCea47368	Additional access-request seen under stress-test Symptoms: Redundant access-request is seen when the gateway is under a stress test. This may affect service. Workaround: There is no workaround.
CSCeb71791	%ISDN-6-CHAN_UNAVAILABLE: msgs seen in stress test Symptoms:%ISDN-6-CHAN_UNAVAILABLE: Interface Se1/0:1:23 Requested Channel 14 is not available is displayed Conditions: This seems to happen under load conditions, and is common if any race conditions occur. Workaround: No workaround is required as the system is not impacted.

Resolved Caveats—Cisco IOS Release 12.2(15)ZK2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZK2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 12 Resolved Caveats for Cisco IOS Release 12.2(15)ZK2

DDTS ID Number	Description
CSCdy32346	Calltracker displays MLPPP calls as PPP. Symptoms: Calltracker records currently display the service type as PPP instead of multilink PPP (MLPPP). Workaround: There is no workaround.
CSCea28285	Attribute[61] shows Virtual with Tcp-clear calls Symptoms: Attribute [61], Nas-Port-Type shows "Virtual" with TCP-Clear calls. This may affect service. Workaround: There is no workaround.
CSCeb62876	No AAA accounting gigawords in not functioning correctly Symptoms: After turning off the **aaa accounting gigawords** command and rebooting the router, it continues to send 64-bit counters in accounting records. These counters also are invalid. Workaround: There is no workaround.
CSCec06617	Getting two Acco. Stop Records when a telnet connection times out Symptoms: Configure the router to send accounting start and stop records for an EXEC connection and configure the command **aaa accounting send stop-record authen fail**. Telnet to the router from any other router. Do not enter anything when the router prompts you to enter a username. After some time, the session times out and prompts "[Connection to <IP Addr> closed by foreign host]". When the Telnet connection times out, two accounting stop records are generated. Workaround: There is no workaround.
CSCec16481	A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default. The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains. Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL: http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml.
CSCec29993	Add RXTYPE_PPPOE to as5400_scattered_fs_protocol - if_as5400_amdp2.h Symptoms: Particles are coalesce when they are CEF switched, because PPPoE is not in the list eligible fast switch protocols. Conditions: This happens for packets passing through PPPoE tunnel. Workaround: There is no workaround.

Table 12 Resolved Caveats for Cisco IOS Release 12.2(15)ZK2 (continued)

DDTS ID Number	Description
CSCec31161	Outgoing LSDO call not forwarded to other SGBP peer if T1s are down Symptoms: Outgoing large scale dial out (LSDO) calls may not be forwarded to other Stack Group Bidding Protocol (SGBP) members from a NAS which has all the trunks down. This happens with an SGBP configuration only when NAS is running Cisco IOS Release 12.2(15)T2. Workaround: There is no workaround.
CSCin52071	L2TP sess cannot be established as PPP says Lower Layer not up Symptoms: Virtual private dialup network (VPDN) sessions cannot be established at the Layer 2 Tunneling Protocol (L2TP) network server (LNS). Conditions: This symptom is observed on a Cisco LNS that is running Cisco IOS Release 12.3 because PPP does not allow packets to be processed. The following debug message appears: `195: ppp4 LCP: Lower layer not up, discarding packet` Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(15)ZK1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)ZK1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 13 Open Caveats for Cisco IOS Release 12.2(15)ZK1

DDTS ID Number	Description
CSCdy32346	Calltracker displays MLPPP calls as PPP Symptoms: Calltracker records currently display the service type as PPP instead of multilink PPP (MLPPP). Workaround: There is no workaround.
CSCea47368	Additional access-request seen under stress-test. Symptoms: Redundant access-request is seen under a stress test. This may affect service. Workaround: There is no workaround.
CSCea70269	Incorrect values for AAA attributes 42,43,52,53 after stress test Symptoms: TCP-clear calls may display incorrect values in authentication, authorization, and accounting (AAA) stop records for attributes 42, 43, 52, and 53. When attributes 42 and 43 are used for billing purposes, this situation may impact service. Conditions: This symptom is observed after a stress test in which more than 600 analog PPP and TCP clear calls are set up and torn down over a period of 12 hours. Workaround: There is no workaround.

Table 13 Open Caveats for Cisco IOS Release 12.2(15)ZK1 (continued)

DDTS ID Number	Description
CSCeb13748	route-map counters not working on FB for policy routing for async ca Symptoms: While testing policy routing on a Cisco AS5850 access server, the route-map counters are not increasing on feature board (FB) for async calls. The ACL counters (for matching entries) are increasing on FB. Route-map counters on RSC are increasing for packets that are punted. Workaround: Use ACL counters.
CSCeb56536	IP pool download fails for dialin user Symptoms: The IP pool download fails for dial-in users. The call is also terminated. Workaround: Use local pools.
CSCeb69182	Router reloads unexpectedly at pm_spe_busyout_cb() Symptoms: A Cisco AS5850 access server may unexpectedly reload on OIR of feature board (FB). This is reproducible. This may impact service. Workaround: There is no workaround.
CSCeb73169	packets for non-mlp non-vp digital calls are not policy routed Symptoms: Policy routing is not working for non multilink non virtual-profile digital calls on the Cisco AS5850 access server. Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(15)ZK1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZK1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 14 Resolved Caveats for Cisco IOS Release 12.2(15)ZK1

DDTS ID Number	Description
CSCdx35399	Need ability to clear clear route-map to clear number of matches This adds support of the **clear route-map counters** command.
CSCdy84543	CEF PBR set default-nexthop or default interface does not work Symptoms: The packets may not get switched to the next default hop with the **set ip default next-hop** command configured. Workaround: There is no workaround.
CSCdz44799	Reverse Telnet Fails with AAA Symptoms: Reverse Telnet session fails when AAA is invoked. Conditions: Reverse Telnet in to the access server port. AAA authorization reverse-access default group is used in the configuration. Workaround: There is no workaround.

Table 14 Resolved Caveats for Cisco IOS Release 12.2(15)ZK1 (continued)

DDTS ID Number	Description
CSCea27261	NAS sends out a unwanted Access request for PTA Symptoms: Network access server (NAS) sends out a unwanted access request for PTA When using VPDN with RADIUS a double RADIUS lookup occurs. This causes a performance hit on the RADIUS server with a large number of additional RADIUS requests. Workaround: There is no workaround.
CSCea28285	Attribute[61] shows Virtual with TCP-clear calls Symptoms: Attribute [61], Nas-Port-Type shows "Virtual" with TCP-Clear calls. This may affect service. Workaround: There is no workaround.
CSCea36327	initiate-to ip x.x.x.x limit y does not work without RPM Symptoms: VPDN session limit that is defined for a VPDN-group does not work without enabling RPM. This may impact provisioning of VPDN session limits for a particular home gateway if RPM is not enabled. Workaround: There is no workaround.
CSCea53451	5850 crashes in cpm_dequeue_calls_list after 4 to 5 hours of stress Symptoms: A Cisco AS5850 access server may reload after 4 to 5 hours of operation. Conditions: This symptom is observed on a Cisco AS5850 access server that is running Cisco IOS Release 12.2(15)T and that has a call load of 8 calls per second. Workaround: There is no workaround.
CSCea64832	NAS reloads with deb resource-poolon and make calls > vpdn-limit Symptoms: A network access server (NAS) reloads when it tries to make calls after the session limit that is configured under the vpdn-group has been exceeded. This may not impact service as the NAS reloads only when resource-pool debugging is enabled. Workaround: Disable resource-pool debugging.
CSCea76989	Spurious memory access at mfcl_vpdn_session_down on clearing MMP cal Symptoms: Spurious memory access is seen on a master network access server (NAS) on clearing the virtual-access interface of MMP calls.This happens only when the Stack Group Bidding Protocol (SGBP) tunnelling protocol is set to default (i.e. L2TP) on master and slave NASes This may not impact service as it does not occur when you clear calls from callers. Workaround: Set the SGBP tunnelling protocol to l2f by configuring **sgbp protocol l2f**.
CSCeb06484	fib sh cef int output on FB indicates dCEF disabled Symptoms: The output of the **sh cef int** command on the feature board (FB) of the Cisco AS5850 access server indicates that dCEF switching is disabled when it is enabled on the RSC. Workaround: There is no workaround.
CSCeb71997	PBR breaks after changing RouteMap on ZK images Symptoms: While testing policy-based routing (PBR) on Cisco IOS Release 12.2(15)ZK, the following problem is observed on the Cisco AS5850. PBR fails after the route-map is changed (dynamically after the call is up). Once the call is terminated and started again, PBR works. Workaround: Do not make changes to route maps while calls are connected.

Table 14 Resolved Caveats for Cisco IOS Release 12.2(15)ZK1 (continued)

DDTS ID Number	Description
CSCeb74981	ip DCEF with PBR not working correctly Symptoms: Packets are not being policy routed. Conditions: Distributed CEF switching is enabled. Workaround: Disable dCEF. Further Problem Description: Policy routing does not working correctly when dCEF is enabled.
CSCin45946	Getting two Acct.STOP Records when a Telnet connection times out Symptoms: Configure the router to send accounting start and stop records for a EXEC connection and configure the **aaa accounting send stop-record authen fail** command. Telnet to the router from any other router. Do not enter anything when it prompts you to enter a username. After some time, it times out and displays "[Connection to <IP Addr> closed by foreign host]". When the Telnet connection times out, two accounting stop records are generated. Workaround: There is no workaround.
CSCin48354	LCP fails to come to open as lower layer not up Symptoms: LCP negotiation fails as a network access server (NAS) discards the packets with message "Lower layer not up, discarding packet." Problem: The ping from the client to NAS fails with an AAA configuration. Workaround: Do not configure anything that causes a virtual profile to be created, including AAA peruser configuration or 'virtual-profile virtual- template' configuration.

Open Caveats—Cisco IOS Release 12.2(15)ZK

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)ZK and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 15 Open Caveats for Cisco IOS Release 12.2(15)ZK

DDTS ID Number	Description
CSCeb70215	Spurious access recorded at vp_fastsend and les_ipfib_switch Symptom: The following traces are seen during the stress tests: vp_fastsend and les_ipfib_switch. Workaround: There is no workaround.
CSCeb71791	%ISDN-6-CHAN_UNAVAILABLE: msgs seen in stress test Symptom: During stress test of a Cisco AS5400, %ISDN-6-CHAN_UNAVAILABLE messages appear. Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(15)ZK

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(15)ZK and describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 16 Resolved Caveats for Cisco IOS Release 12.2(15)ZK

DDTS ID Number	Description
CSCdz44203	Dynamic Dialer map not created with aaa authentication if-needed Symptoms: The following occur: • The interface connection to a Cisco AS5350 using a post dial terminal window for authentication may not be able to ping the Cisco AS5350 after connecting. • No output packets can be seen on the asynchronous interface to which the user connects. Condition: This problem only occurs with **aaa authentication ppp** <*list*> **if-needed** configured. The problem is that a dynamic dial map is not created for the user. This can be seen with the **show dialer map** command. Workaround: Reconfigure the router to use virtual-profiles, or remove **if-needed** from the AAA authentication command.
CSCea48500	Attribute 46 may be of value 0 for async calls in n/w stop records. Symptoms: Attribute 46 (indicating the account session time) may show a value of zero under the network stop records for asynchronous calls. Conditions: This symptom is observed on a Cisco universal access server. If you use network stop records for billing purposes, the symptom may affect the service. Workaround: There is no workaround.
CSCea53600	authorization failure for terminal login call with per-user DNS/WINS Symptoms: Authorization may fail for a terminal server login call. Conditions: This symptom is observed on a Cisco AS5400 when authorization occurs through a RADIUS-assigned Domain Name System (DNS) server or Microsoft Windows Internet Naming Service (WINS) server. Workaround: There is no workaround.
CSCea61814	bearer capability changed for outgoing hairpinned call Symptom: The bearer capability is changed for outgoing hairpinned calls. Workaround: There is no workaround.
CSCea79607	First Outgoing CONFREQ not received by Windows PPP clients Symptom: First outgoing CONFREQ is not received by the PPP Windows DUN client. Conditions: LCP negotiation takes awhile. Workaround: Make all connections into the NAS dedicated by configuring **async mode dedicated** under the Group-Async interface.
CSCeb08802	DS0 info of CAS T1s not reported in radius accounting Symptom: Radius accounting for CAS T1s may not be reported on the DS0 information. Conditions: This occurs on a Cisco AS5400 with CAS T1s provisioned. Workaround: There is no workaround.

Table 16 Resolved Caveats for Cisco IOS Release 12.2(15)ZK (continued)

DDTS ID Number	Description
CSCeb08838	Progress code reported incorrect for TCPclear sessions Symptom: Radius accounting progress code for successful TCPclear (AOL P3) sessions may be reported intermittently as value "47" - "Terminal-server authentication started" Conditions: This occurs on a Cisco AS5400 and Cisco AS5800 that are configured for TCPclear. Workaround: There is no workaround.
CSCeb30519	Per-user configuration not applied for EXEC authenticated users Symptom: When using RADIUS to authorize dial-in PPP users, some authorization attributes may not be applied correctly for users who dial in and are EXEC authenticated. Workaround: Disable EXEC login and configure the async interfaces for **async mode dedicated**.

This document is to be used in conjunction with the documents listed in the "Inheritance Information" section on page 2.