



Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(15)ZJ5

April 26, 2004

These release notes describe new features and significant software components for the Cisco 1700 series routers that support the Cisco IOS Release 12.2 T, up to and including Release 12.2(15)ZJ5. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the [Cross-Platform Release Notes for Cisco IOS Release 12.2 T](#) located on Cisco.com and the Documentation CD.

For a list of the software caveats that apply to Release 12.2(15)ZJ5, see the “[Caveats](#)” section on page 32, and the online [Caveats for Cisco IOS Release 12.2 T](#) document. The caveats document is updated for every 12.2 T maintenance release and is located on Cisco.com and the Documentation CD.

Contents

These release notes discuss the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 6](#)
- [Caveats, page 13](#)
- [Related Documentation, page 22](#)
- [Obtaining Documentation, page 23](#)
- [Obtaining Technical Assistance, page 24](#)
- [Obtaining Additional Publications and Information, page 25](#)



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

Copyright © 2003. Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Release 12.2(15)ZJ5 and includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Set Tables, page 4](#)

Memory Requirements

Table 1 describes the memory requirements for the Cisco IOS feature sets supported by the Cisco IOS Release 12.2(15)ZJ5 on the Cisco 1700 series routers.

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 1751	Cisco 1710 IOS IP/VOX PLUS	IP/VOX PLUS	c1710-bk9no3r2sy-mz	16 MB	64 MB
Cisco 1751-V and Cisco 1760	Cisco 1700 IOS IP/VOX PLUS	IP/VOX PLUS	c1700-sv8y-mz	16 MB	64 MB
	Cisco 1700 IOS IP/ADSL/VOX PLUS	IP/ADSL/VOX PLUS	c1700-sv8y7-mz	32 MB	96 MB
	Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS IPSEC 56	IP/ADSL/VOX/FW/IDS PLUS IPSEC 56	c1700-k8o3sv8y7-mz	32 MB	96 MB
	Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS IPSEC 3DES	IP/ADSL/VOX/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sv8y7-mz	32 MB	96 MB

Hardware Supported

Cisco IOS Release 12.2(15)ZJ5 supports the following Cisco 1700 series routers:

- Cisco 1751 and 1751-V router
- Cisco 1760

The Cisco 1751, Cisco 1751-V, and 1760 routers run data or data-and-voice images, providing digital and analog voice support.

For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1700 series routers, which are available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1700 Series Routers: <platform_name>

Determining the Software Version

To determine which version of Cisco IOS software is currently running on your Cisco 1700 series router, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number.

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-NY-MZ), Version 12.2(15)ZJ5, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.2(15)T1
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer the *Software Installation and Upgrade Procedures* located at 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. Release 12.2(15)ZJ3 supports the same feature sets as Releases 12.2 and 12.2(8)T, but Release 12.2(15)ZJ3 includes new features supported by the Cisco 1700 series routers.



Caution

The Cisco IOS images with strong encryption (including, but not limited to, 168-bit [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 will likely require an export license. Customer orders can be denied or subject to delay as a result of United States 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.

Table 2 and Table 3 list the features and feature sets supported in the Cisco IOS Release 12.2(15)ZJ5.

The tables use 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)ZJ” means that the feature was introduced in 12.2(15)ZJ. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.



Note

These feature set tables contain only a selected list of features, which are cumulative for Release 12.2(15)*nm* early deployment releases only (*nm* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in the [Cross-Platform Release Notes for Cisco IOS Release 12.2 T](#) and Release 12.2 T Cisco IOS documentation.

Table 2 Feature List by Feature Set for Cisco 1751 Router

Feature	In	Feature Set
		IP/VOX PLUS
SIP Cisco Survivable Remote Site Telephony (SRST)	12.2(15)ZJ	Yes
Cisco IOS Telephony Service Version 3.0	12.2(15)ZJ	Yes
SRST: Cisco Survivable Remote Site Telephony Version 3.0	12.2(15)ZJ	Yes

Table 3 Feature List by Feature Set for Cisco 1751-V and 1760 Routers

Feature	In	Feature Set		
		IP/ADSL/VOX PLUS	IP/ADSL/VOX/ FW/IDS PLUS IPSEC 56	IP/ADSL/VOX/ FW/IDS PLUS IPSEC 3DES
SIP Cisco Survivable Remote Site Telephony (SRST)	12.2(15)ZJ	Yes	Yes	Yes
Cisco IOS Telephony Service Version 3.0	12.2(15)ZJ	Yes	Yes	Yes
SRST: Cisco Survivable Remote Site Telephony Version 3.0	12.2(15)ZJ	Yes	Yes	Yes

New and Changed Information

The following sections list the new software features supported by the Cisco 1700 series routers for Release 12.2(15)ZJ5.

New Software Features in Release 12.2(15)ZJ5

The Cisco IOS Release 12.2(15)ZJ5 supports the same software features that are supported in the Cisco IOS Release 12.2(15)ZJ and the Cisco IOS Release 12.2(15)ZJ3.

New Software Features in Release 12.2(15)ZJ3

The following sections describe the new software features supported by the Cisco 1700 series routers for Release 12.2(15)ZJ3.

Cisco CallManager Express 3.0

The Cisco CallManager Express (Cisco CME) is the new name for the product previously known as Cisco IOS Telephony Services (Cisco ITS). In addition to the features introduced in the Cisco IOS Release 12.2(15)ZJ, the current release adds support for the Cisco Wireless IP Phone 7920 when it registers with Cisco CME as a Cisco IP Phone 7960. In this release, there are a set of features that are not supported on the Cisco Wireless IP Phone 7920 (intercom and paging to the phones are the two most prominent). These features and others will be added in future releases.

For more information, refer to the Cisco CallManager Express 3.0 System Administrator Guide at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/index.htm>

A new command reference that documents all the Cisco CallManager Express 3.0 commands is located in the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/cme30cr/index.htm>

New Software Features in Release 12.2(15)ZJ2

The Cisco IOS Release 12.2(15)ZJ2 supports the same software features that are supported in the Cisco IOS Release 12.2(15)ZJ.

New Software Features in Release 12.2(15)ZJ1

The Cisco IOS Release 12.2(15)ZJ1 supports the same software features that are supported in the Cisco IOS Release 12.2(15)ZJ.

New Software Features in Release 12.2(15)ZJ

The following sections describe the new software features supported by the Cisco 1700 series routers for Release 12.2(15)ZJ.

SIP Survivable Remote Site Telephony (SRST)

The SIP Survivable Remote Site Telephony (SRST) feature describes SRST functionality for Session Initiation Protocol (SIP) networks. The SIP-SRST provides backup to an external SIP proxy server by providing basic registrar and redirect services. These services are used by a SIP IP phone in the event of a WAN connection outage and the SIP phone is unable to communicate with its primary SIP proxy. The SIP-SRST device also provides PSTN gateway access for placing and receiving PSTN calls.

SIP-SRST provides four new features:

- SIP Registrar

A local SIP gateway that becomes the SIP registrar acts as a backup SIP proxy or redirector, and accepts SIP register messages from SIP phones. It becomes a location database of local SIP IP phones that are set up for dual-registration. Dual-registration allows SIP IP phones to simultaneously register with both their primary and fallback registrar devices. That is, when a SIP IP phone registers with a SIP-SRST gateway, it simultaneously registers with the main proxy and SIP redirect server for coverage in case of WAN failure. A registrar accepts SIP register requests and dynamically builds Voice over IP (VoIP) dial peers allowing the Cisco IOS Voice Gateway software to route calls to SIP phones.

- Backup registrar service to SIP IP phones

Backup registrar service to SIP IP phones can be provided by configuring a voice register pool on SIP gateways. The voice register pool configuration provides registration permission control and can also be used to configure some dial peer attributes that are applied to the dynamically created VoIP dial peers when SIP phone registrations match the pool.

- Call redirect enhancement to support calls between SIP IP phones through the Cisco IOS Voice Gateway

The call redirect enhancement supports calls from a local SIP phone to another local SIP phone through the Cisco IOS Voice Gateway. Prior to this enhancement, an attempt by a SIP phone to contact another local SIP phone using the Cisco IOS Voice Gateway as if it were a SIP proxy or redirect server would fail. However, now the Cisco IOS Voice Gateway can act as a SIP redirect server. The voice gateway responds to the originator with a SIP redirect message, allowing the SIP phone that originated the call to establish a call to its destination.

- Sending 300 Multiple Choice messages

Prior to the Cisco IOS Release 12.2(15)ZJ, when a call was redirected, the SIP gateway would send a “302 Moved Temporarily” message. The first longest match route on a gateway (dial-peer destination pattern) was used in the *Contact* header of the 302 message. With the Cisco IOS Release 12.2(15)ZJ, if multiple routes to a destination exist for a redirected number (multiple dial peers are matched), the SIP gateway sends a “300 Multiple Choice” message and the multiple routes in the *Contact* header are listed.

Cisco IOS Telephony Services Version 3.0

The Cisco IOS Telephony Services (ITS) Version 3.0 delivers the next-generation ITS feature set.

The Cisco ITS Version 3.0 supports the following enhancements:

- ITS setup tool for quick installation
The ITS setup tool provides a question-and-answer interface that allows the user to set up an entire Cisco ITS system automatically.
- Automatic assignment of free extension numbers to new IP phones
The **auto assign** command specifies a range of extension numbers to which newly discovered IP phones are automatically assigned. This method is useful when you have a phone setup in which each phone is assigned a separate, unique extension number.
- Call pickup and call pickup groups
Call pickup allows phone users to retrieve calls from other extension numbers by using the *PickUp* soft key and dialing the ringing number. When extensions are assigned to pickup groups, other members of the group can retrieve incoming calls using fewer keystrokes.
- Night service
When night service is active, incoming calls to designated night-service extension numbers will also ring on other phones that are designated as night-service phones. Phone users at the other phones can use call pickup to retrieve the incoming calls.
- Call-blocking (toll bar) based on time of day, day of week, or date
Call blocking to prevent the unauthorized use of phones is implemented by matching calls to a specified digit pattern during a specified time period. Up to 32 patterns of digits can be specified. Individual phones can be exempted from call blocking, and individual user logins can override call blocking if they are configured.
- Hunt groups
Ephone hunt groups provide the ability to direct incoming calls for a specific number (the ephone hunt group pilot number) to a defined group of extensions. Incoming calls are redirected on busy or no answer from extension to extension in the list until they are answered or they reach the number that is defined as the final number.
- Secondary dial tone
Secondary dial tone is generated when a phone user dials a predefined digit. The tone terminates when additional digits are dialed. For example, one can configure a secondary dial tone to be heard after the number 9 is dialed to reach an external line.
- Cisco IP Phone 7902G Support
The Cisco IP Phone 7902G, is a cost effective, entry level IP phone addressing the voice communications needs of a lobby, laboratory, manufacturing floor, or hallway—or other areas where only basic calling capability is required. For further information, go to Cisco.com and click **Products & Service, IP Phone, Cisco 7900 Series IP Phones, Product Literature, and Data Sheets** or go to http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7902/index.htm.

- Cisco IP Phone 7912G Support

The Cisco IP Phone 7912G provides core business features and addresses the communication needs of a cubicle worker who conducts low to medium telephone traffic. The Cisco IP Phone 7912G offers four dynamic soft keys that guide a user through call features and functions. For further information, go to Cisco.com and click **Products & Service, IP Phone, Cisco 7900 Series IP Phones, Product Literature**, and **Data Sheets**.

- Speed dial

Three types of speed dial are available:

- On multi-button phones, the buttons that are not used for extensions can be programmed as speed dial buttons.
- Local speed dial numbers are common to all phone users in an ITS system. Phone users access the list of local speed dial numbers from the *Directories* button.
- Personal speed dial numbers are specific to individual phones. Phone users access their list of personal speed dial numbers from the *Directories* button.

- Account code entry

The Cisco IP Phone 7940 and Cisco IP Phone 7960 users can enter account codes during call setup or while connected to an active call, using the *Acct* soft key. Account codes are inserted into call detail records (CDRs) on the ITS router for later interpretation by billing software.

- Callback busy subscriber

This feature allows callers who dial a busy extension number to request a callback from the system when a called number that was busy is free. Callers can also request callbacks for extensions that do not answer and the system will notify them after the called phone is next used.

This feature is available only on Cisco IP Phone 7940 and Cisco IP Phone 7960.

- Do not disturb

Do not disturb (DND) service is enabled using a soft key on a Cisco IP Phone 7940 or a Cisco IP Phone 7960. When DND is enabled, incoming calls do not ring on the phone, but do provide visual alerting and call information and can be answered if desired. A display message indicates that DND feature is enabled. Call forwarding on busy and no answer operates the same as without DND.

- Several international languages and call-progress tone sets are newly supported, as well as international date and time formats. The set of supported languages varies by phone type.

- Call-forward-all soft key on the Cisco IP phones

- Flash soft key for hookflash functionality for the PSTN

Certain PSTN services, such as three-way calling and call waiting, require hookflash intervention from a phone user. A new soft key *Flash* is introduced to provide this functionality for Cisco IP Phone 7940 and Cisco IP Phone 7960 users on Foreign Exchange Office (FXO) lines attached to the ITS system. The *Flash* soft key is enabled using the **fxo hook-flash** command.

- Dual-line mode

Dual-line extensions are available to handle call-waiting, call transfer, or conferencing using a single button.

- Extension overlays for better call handling and distribution

An extension (ephone-dn) overlay allows more than one ephone-dn to use the same physical line button on an IP phone. Overlaid ephone-dns can be used to receive incoming calls and place outgoing calls.

- ITS GUI enhancements

The Cisco ITS GUI provides a web-based interface to manage most ITS system-wide and phone-based features. In particular, the GUI facilitates the routine adds and changes associated with employee turnover, allowing these changes to be performed by non-technical staff.

The ITS GUI provides three levels of access to support the following user classes:

- System administrator—Able to configure all systemwide and phone-based features. This person is familiar with the Cisco IOS software and VoIP network configuration.
- Customer administrator—Able to perform routine phone adds and changes without having access to systemwide features. This person does not have to be trained in the Cisco IOS software.
- Phone user—Able to program a small set of features on his or her own phone and search the ITS directory.

- Label support

The label support feature allows to enter a meaningful text string to view in the display adjacent to an extension button on an IP phone rather than the extension number that is associated with that button.

- Busy lamp monitor and direct station select

For multi-button phones and expansion modules, the buttons for extensions that are shared with other phones can be designated as monitor buttons, which show the status of those extensions on the other phones. When not in use, a monitor line can be used with the *Transfer* soft key to quickly transfer a call.

- Phone directory entry

The Cisco ITS system automatically creates a local phone directory based on the telephone numbers that are assigned during the configuration of extensions and phones. Additional entries to the local ITS directory can be made using the **directory entry** command.

- Silent and feature ring options

The silent ring feature allows to designate phone buttons that do not emit an audible ring when they receive incoming calls. Although this feature is supported by all phone types, it is most useful on phone buttons that are used to display the activity of shared lines, which are typically found on the Cisco IP Phone 7960 and Cisco IP Phone Expansion Module 7914.

- New and modified commands

About 35 new and modified commands are described in the Command Reference at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/its30cmd.htm>

For more information, refer to the *Cisco ITS System Administrator Guide Version 3.0* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/index.htm>

SRST: Survivable Remote Site Telephony Version 3.0

The Cisco SRST Version 3.0 feature supports the following enhancements:

- Cisco IP Phone 7902G Support

The Cisco IP Phone 7902G, is a cost effective, entry level IP phone addressing the voice communications needs of a lobby, laboratory, manufacturing floor, or hallway—or other areas where only basic calling capability is required. The Cisco IP Phone 7902G is a single-line IP phone, with fixed feature keys that provide one-touch access to redial, transfer, conference, and voice-mail access features. Consistent with other Cisco IP phones, the Cisco IP Phone 7902G supports in-line power, which allows the phone to receive power over the LAN. This capability gives the network administrator centralized power control, translating into greater network availability.

For further information, go to Cisco.com and click **Products & Service, IP Phone, Cisco 7900 Series IP Phones, Product Literature**, and **Data Sheets** or refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7902/index.htm

- Cisco IP Phone 7912G Support

The Cisco IP Phone 7912G provides core business features and addresses the communication needs of a cubicle worker who conducts low to medium telephone traffic. The Cisco IP Phone 7912G offers four dynamic soft keys that guide a user through call features and functions. The graphic capability of the display provides a rich user experience by providing calling information and intuitive access to features.

The Cisco IP Phone 7912G supports an integrated Ethernet switch, providing LAN connectivity to a collocated PC. In addition, the Cisco IP Phone 7912G supports in-line power, which allows the phone to receive power over the LAN. This capability gives the network administrator centralized power control, translating into greater network availability. The combination of in-line power and Ethernet switch support reduces cabling needs to a single wire to the desktop.

For further information, go to Cisco.com and click **Products & Service, IP Phone, Cisco 7900 Series IP Phones, Product Literature**, and **Data Sheets**.

- Customized system message for Cisco IP phones

The display message that appears on Cisco IP Phone 7905G, Cisco IP Phone 7910, Cisco IP Phone 7940, and Cisco IP Phone 7960 when they are in fallback mode can be customized. The new system message command allows to edit these display messages on a per router basis.

- Consultative call transfer using the H.450.2 standard

The Cisco SRST Version 1.0 allowed only blind call transfers, in which a transferring party did not have the ability to announce or consult with a destination party before transferring a call. The Cisco SRST Version 1.0 used a Cisco SRST proprietary mechanism to perform these blind transfers. The Cisco SRST Version 3.0 adds the ability to perform call transfers with consultation or blind transfer using the ITU-T H.450.2 standard for H.323 calls.

- Dual-line mode

A new keyword has been added to the **max-dn** command allows to set IP phones to dual-line mode. Each dual-line IP phone has one voice port and two channels to handle two independent calls. This mode enables call waiting, call transfer, and conference functions on a single ephone-dn. Dual-line mode works with all phone types. The **max-dn** command is a global command that affects all IP phones on an Cisco SRST router.

- European date formats
The date format on Cisco IP phone displays can be configured with the following two additional formats:
 - yy-mm-dd (year-month-day)
 - yy-dd-mm (year-day-month)
 - Music-on-hold for multicast from Flash files
The Cisco SRST can be configured to support continuous multicast output of music-on-hold (MoH) from a Flash MoH file in Flash memory.
 - Ringing timeout default
A ringing timeout default can be configured for extensions on which no-answer call forwarding is not enabled. Expiration of the timeout causes incoming calls to return a disconnect code to the caller. This mechanism provides protection against hung calls for inbound calls received over interfaces such as Foreign Exchange Office (FXO) that do not have forward-disconnect supervision.
 - The **show ephone** command
The **show ephone** command has been enhanced to display the following:
 - Configuration and status of phones of the specified type (new keywords: 7914, 7905, 7935, ATA)
 - Status of all phones with the call-forwarding all calls (CFA) feature enabled on at least one of their DNs (new keyword: cfa)
 - Syslog messages for phone registrations
Diagnostic messages are added to the system log whenever a phone registers or unregisters from the Cisco SRST.
 - Three-party G.711 ad hoc conferencing
The Cisco SRST supports three-party ad hoc conferencing using G.711. For conferencing to be available, an IP phone should have a minimum of two lines connected to one or more buttons.
 - Additional language support on the Cisco IP phones
Display support for four additional languages is added to a select group of the Cisco IP Phones.
 - New and modified commands
About 10 new and modified commands are described in the Command Reference at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/srs30/srs_cmds.htm
- For further information about the SRST Version 3.0 features, refer to the *Cisco SRST System Administrator Guide Version 3.0* at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zj15/itsv30/index.htm>

New Software Features in Release 12.2(15)T

For information regarding the features supported in the Cisco IOS Release 12.2 T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/index.htm>

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:

Service & Support: Technical Documents: Cisco IOS Software: Release 12.2: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.2T)

Caveats

Caveats describe unexpected behavior or defects in the Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Release 12.2 T are also in Release 12.2(15)ZJ3. For information on caveats in the Cisco IOS Release 12.2 T, refer to the *Caveats for Cisco IOS Release 12.2 T* document. For information on caveats in the Cisco IOS Release 12.2, refer to the *Caveats for Cisco IOS Release 12.2* document. These documents list severity 1 and 2 caveats; the documents are located on Cisco.com and the Documentation CD.



Note

If you have an account with 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 **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Resolved Caveats for Release 12.2(15)ZJ5

The following sections lists the open caveats for the Cisco IOS Release 12.2(15)ZJ5.

- CSCdz30977

Modem pass-through: Option to eliminate glitch for low-speed modem.

Symptoms: The V.22B modem connections may not work reliably when modem pass-through is configured.

Workaround

None.

- CSCed93836

Modifications needed to syn rst packet response.

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>.

- CSCdz84583

The Cisco IOS firewall allowing forged packets for a session initiated from inside.

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>.

- CSCeb52066

NAT: Provide an API to get the pre-NAT transferred TCP Seq/Ack Numbers.

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>.

- CSCed35253

Router crash due to corrupted data in list with Cisco IOS-firewall.

Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

Workaround

Disable IP Inspect and IDS.

- CSCec59206

Bus error in NAT translating RSHELL packets.

Symptoms: A router may reload unexpectedly because of a bus error when it accesses a low address during the translation of TCP port 514.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(5) and that is configured for Network Address Translation (NAT).

Workaround

Prevent the translation of TCP port 514.

Open Caveats for Release 12.2(15)ZJ3

The following sections lists the open caveats for the Cisco IOS Release 12.2(15)ZJ3.

- CSCin51176

The outbound Voice over IP (VoIP) dialpeer is not selected with called-number alone.

Workaround

None.

- CSCin46584
IP-IP gateway does not transfer the information elements (IEs) completely.

Workaround

None.

- CSCeb67032
CFALL after a full-blind transfer between ITSs not working.

Workaround

None.

- CSCin55495
After sending PROGRESS message with progress indicator, the originating gateway is not sending the CONNECT message.

Workaround

Configure the “default.c.old” application on the terminating gateway.

Resolved Caveats for Release 12.2(15)ZJ3

The following sections lists the resolved caveats for the Cisco IOS Release 12.2(15)ZJ3.

- CSCin51788
“progress_ind connect” progress indicator is not sent from terminating gateway to originating gateway.

Workaround

None.

- CSCdx95698
No ringback on transfer on using interactive voice response (IVR) clid_authn_collect.

Workaround

None.

- CSCeb65637
Unable to set the H.323 call identifier from Tcl interactive voice response (IVR) script.

Workaround

- Setup a call with an incoming leg.
- Use the command **set callinfo(newguid)** to force the call setup to generate a new conferenceID and call identifier. This assumes that the generated GUID does not affect the billing system or the remote endpoint.

Example:

```
set callinfo(newguid) true
leg setup $dest_nr callinfo
```


Resolved Caveats for Release 12.2(15)ZJ1

The following sections lists the resolved caveats for the Cisco IOS Release 12.2(15)ZJ1.

- CSCea22283

Wrong voice mail box selected when call forwarded across multiple phones.

Symptoms: The caller reaches the original destination's voicemail when the forwarded-to destination is not available.

Conditions: If a call is forwarded across multiple IP phones, the voicemail box selected is that of the original called number.

For example: A calls B and the call is forwarded to C. C does not answer and the call gets forwarded to B's voice mail (instead of C's voicemail).

Workaround

None.

- CSCuk42484

Wrong cause value when transferring to busy/unallocated number.

Symptoms: The wrong cause value is provided when transferring a call to an unallocated or busy destination.

Conditions: This behavior can occur when an incoming call VoIP call is handled by the app-h450-transfer.2.0.0.3.tcl application. If the transfer target is telephony or ITS destination that is busy or unallocated, and if there is a VoIP dial-peer that matches the transfer target phone number, the gateway will place an outbound VoIP call instead of disconnecting the incoming call with the appropriate cause code. In this case, the final cause value returned to the incoming call will depend on the outgoing call setup request.

Workaround

None.

- CSCeb01098

Release source not being set by new session application.

Symptoms: The release sources reported in the Remote Authentication Dial-In User Service (RADIUS) accounting record or the gateway's call history record for the incoming and outgoing legs do not match. This behavior does not affect the voice call.

Conditions: This behavior may occur when the default voice application handles the incoming call.

Workaround

Configure **application default.c.old** command on the incoming dial-peer used for the call.

- CSCuk43681

The call is mishandled when calling an unallocated number.

Symptoms: Congestion tone is not provided to the caller when a call setup attempt fails with cause 'Temporary Failure' (41 / 0x29).

Workaround

None.

- CSCdz71127

Corrupted packet can cause input queue wedge.

Cisco routers and switches running the Cisco IOS software, and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtm>

Open Caveats for Release 12.2(15)ZJ1

The following sections lists the open caveats for the Cisco IOS Release 12.2(15)ZJ1.

- CSCuk41974
Ringback tone and fast busy tone not as per the **cptone** command configured.
Symptoms: The ringback tone provided during alerting, and the fast busy tone provided at the end of the call is not according to the **cptone** command configured on the gateway under the voice port.
Workaround
None.
- CSCin46584
IP-IP gateway does not transfer the IEs completely.
Symptoms: An INFO message received after CONNECT is not forwarded to the other call leg.
A NOTIFY message received before CONNECT is not forwarded to the other call leg.
Conditions: This behavior occurs when the default session application is used to process the call.
Workaround
Configure **application session** command on the incoming dial-peer.
- CSCea65197
No fast busy when SIP AA trigger is disabled.
Symptoms: The user is disconnected without any busy tones when transferred to unreachable destination.
Conditions: This behavior can occur when the transferer uses SIP BYE/ALSO to transfer the call and the transfer target is an invalid or unassigned number.
Workaround
None.
- CSCeb22796
Transferer leg not getting released for SIP call.
Symptoms:
ITS-A----VoIP(SIP)----CSPS----ITS-B
IPPhone-A1 calls IPPhone-B1, call connected
IPPhone-B1 transfers IPPhone-A1 to IPPhone-A2 or FXS-A2 on alerting

The call is transferred. IPPhone-A1 and IPPhone-A2 or FXS-A2 can talk, but, IPPhone-B1 does not get released cleanly. Instead, it hears a fastbusy tone and displays unknown number.

SIP messages show that the call transaction leg does not exist.

Conditions: This behavior can occur when the transferee and transfer-to endpoints are attached to the same gateway and the transfer is committed during alerting.

Workaround

None.

- CSCeb27770

Ephone keeps ringing when disc with PI is received.

Symptoms:

ephone — Cisco 1760 ITS — BRI — PSTN

PSTN calls ephone, PSTN hangs up before ephone answers.

PSTN sends Disconnect with PI = 8, ephone keeps on ringing

Workaround

Configure **disc_pi_off** command on the voice-port.

- CSCeb37176

Caller-ID is wrongly updated in Caller-ID block situations.

Symptoms: The remote party display information is not updated properly after a call transfer.

Conditions: IP Phone A1 calls IP Phone B1 across VoIP. A1 blocks caller-id presentation by dialing *123 before dialing the destination digits. IP Phone B1 correctly displays "Private".

For a transfer commit while alerting, the following behavior is seen:

- a. IP Phone A1 presses the transfer button and dials IP Phone A2 (which is on the same gateway as A1).
- b. IP Phone A2 rings, then IP Phone A1 presses transfer.
- c. When IP Phone A2 answers, IP Phone A2 and IP Phone B1 are connected successfully and:
IP Phone B1 sees IP Phone A2's number (as expected).
IP Phone A2 changes display from "From IP Phone A1" to "From Private" instead of "From IP Phone B1".

For a transfer commit after connect, the following behavior is seen:

- a. IP Phone A1 presses the transfer button and dials IP Phone A2 (which is on the same gateway as A1).
- b. IP Phone A2 answers.
- c. On IP Phone A1 there are 2 displays:
To IP Phone B1
To IP Phone A1 and IP Phone A2's phone number (incorrect)
- d. On pressing transfer:
IP Phone B1 sees IP Phone A2's number
IP Phone A2 changes display from "From IP Phone A1" to "From Private" instead of "From IP Phone B1".

Workaround

None.

Open Caveats for Release 12.2(15)ZJ

The following sections lists the open caveats for the Cisco IOS Release 12.2(15)ZJ.

- CSCea38543

Cisco IP Phone 7902 as XOR cannot make consult-transfer on alerting.

Cisco IP Phone 7902 commit consult transfer at alerting does not work. The Cisco IP Phone 7902 seems to ignore the commit event when pressed in alerting state.

Workaround

- Use blind transfer.
 - Finish the consult call and hang-up or press transfer to commit the consult call properly.
- CSCea93616

A call going through multiple transfers (consult and blind) fails.

Workaround

- Do not chain the transfer.
 - Commit the transfer in the order consult call was placed.
- CSCea22283

Wrong voice mail box selected when call forwarded across multiple phones.

Workaround

Do not chain the forward. Set the forwarding number to voice mail directly, or to a PSTN number (cell phone) since in the latter case, one would get the PSTN to do the forwarding to the respective PSTN's (cell) voice mail.

- CSCuk43724

H.225 messages are not forwarded on the VoIP network on PRI/BRI interface.

After the caller dials the access code of the PRI/BRI link, the number is dialed and an incoming call arrives at the Cisco IOS voice gateway. The gateway has to place an outbound H.323 call to the destination. Instead, a second dial tone is provided on the phone for 15 sec, after which the call is terminated. This behavior occurs when the incoming telephony call arriving at the voice gateway uses overlap receiving and provides complete information in an INFO message following the SETUP message.

Workaround

Configure **application session.c.old** command on the incoming plain old telephone service (POTS) dial peer of the gateway.

- CSCea20968

IVR applications on the outbound dial-peer not getting triggered.

An incoming call to a Cisco IOS voice gateway is handled by the default voice application. If this application places an outbound call which matches a dial-peer that has an outbound application configured, the call handoff to the outbound application will fail.

Workaround

None.

- CSCeb01098

Release Source not being set by new session application.

Workaround

Configure **application session.c.old** on the incoming dial peer used for the call.

- CSCuk42484

Wrong cause value when transferring to busy/unallocated number.

Workaround

None.

- CSCuk41974

Ringback tone and fast busy tone not as per the cptone configured.

Workaround

None.

- CSCuk42727

E_DSM_DSP_PROTOCOL_ERROR during fax pass through call.

Workaround

None.

Resolved Caveats for Release 12.2(15)ZJ

The following sections lists the resolved caveats for the Cisco IOS Release 12.2(15)ZJ.

- CSCea02355

Rare IP packets may cause input queue wedge.

Cisco routers and switches running the Cisco IOS software, and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtm>

Related Documentation

The following sections describe the documentation available for the Cisco 1700 series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration 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.

Use these release notes with the documents listed in the following sections:

- [Release-Specific Documents](#)
- [Platform-Specific Documents](#)

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(15)ZJ3. They are located on Cisco.com and the Documentation CD (under the heading Service & Support):

- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*, click this path:
Technical Documents: Cisco IOS Software: Release 12.2: Release Notes: Cisco IOS Release 12.2 T
- To reach product bulletins, field notices, and other release-specific documents, click this path:
Technical Documents: Product Bulletins
- To reach the *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2, click this path:
Technical Documents: Cisco IOS Software: Release 12.2: Caveats



Note

If you have an account with Cisco.com, you can also use the Bug Toolkit to find selected caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com, and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to Cisco 1700 series routers are available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1700 Series Routers: <platform_name>

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

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

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

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

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private Internets and Intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)
partnership relationship between Cisco and any other company. (0711R)

Copyright © 2004, Cisco Systems, Inc. All rights reserved.