

Cisco Security Advisory: Cisco Telnet Denial of Service Vulnerability

Document ID: 61671

Advisory ID: cisco-sa-20040827-telnet

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

Revision 2.4

Last Updated 2004 December 31 1800 UTC (GMT)

For Public Release 2004 August 27 1000 UTC (GMT)

Please provide your [feedback](#) on this document.

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: INTERIM](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS)[®] may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Data Link Switching (DLSw) and protocol translation connections may also be affected. Telnet, reverse telnet, RSH, SSH, DLSw and protocol translation sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding (excluding DLSw and protocol translation per above), routing protocols and all other communication to and through the device are not affected.

Cisco has made free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

This vulnerability is documented in Cisco bug ID [CSCef46191](#) ([registered](#) customers only) .

This Advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

This vulnerability affects all Cisco devices that permit access via telnet or reverse telnet. Any IOS train without specific fixed releases listed in the [Software Versions and Fixes](#) section should be considered vulnerable.

IOS Release trains confirmed to be affected are 9.x, 10.x, 11.x and 12.x .

Products Confirmed Not Vulnerable

Cisco products that do not run IOS are not affected.

Details

Telnet, RSH and SSH are used for remote management of Cisco IOS devices. The SSH protocol is also used for Secure Copy (SCP), which allows an encryption-protected transfer of files to and from Cisco devices.

Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network. It serves as an alternative to source-route bridging (SRB), a protocol for transporting SNA and NetBIOS traffic in Token Ring environments that was widely deployed before the introduction of DLSw.

For more information on DLSw, refer to the following URL:

<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/DLSw.html>

Protocol translation is a method to connect a host running one protocol (such as Telnet with TCP/IP) to a host running another protocol (such as LAT). This process allows devices running dissimilar protocols such as X.25 and TCP/IP to communicate.

For more information on protocol translation, refer to the following URL:

http://www.cisco.com/en/US/docs/ios/11_0/access/connection/guide/xptservs.html

Services operating over IPv4 and IPv6 are similarly affected.

HTTP is also used for management of certain Cisco devices. IOS versions prior to 12.2(15)T include HTTP server version 1.0, which, if configured, will be unresponsive on a device that is under exploitation. IOS versions after and including 12.2(15)T include HTTP server version 1.1, which is unaffected.

To determine the version of the IOS HTTP server included with the IOS image, the command **show subsys name http** can be used (the **show subsys** command requires enable access to execute):

```
Router# show subsys name http

Class          Version
http          Protocol  1.001.001
```

The above output shows that HTTP server version 1.1 is included.

```
Router# show subsys name http

          Class      Version
http     Protocol    1.000.001
```

The above output shows that HTTP server version 1.0 is included.

Reverse telnet is a feature that allows you to telnet to a Cisco device and then connect to a third device through an asynchronous serial connection; this configuration is often referred to as providing 'console server' functionality for connected devices such as hosts and router/switches as a form of out-of-band (OOB) management. For more information on reverse telnet, consult the following documents:

http://www.cisco.com/en/US/docs/ios/12_0/dial/configuration/guide/dcrtelnt.html

http://www.cisco.com/en/US/docs/ios/11_3/dial/configuration/guide/dcrtelnt.html

Cisco devices that are operating as a reverse telnet server may have ports open in the ranges of:

- 2001 to 2999
- 3001 to 3099
- 6001 to 6999
- 7001 to 7099

After a specially crafted TCP connection to an IOS device on TCP port 23 or the reverse telnet ports listed above, all subsequent telnet, reverse telnet, RSH (TCP port 514), SSH, SCP (SSH and SCP use TCP port 22), DLSw (TCP ports 2065 through 2067), protocol translation, and in some cases HTTP (TCP port 80) connections to the device experiencing exploitation will be unsuccessful. Any telnet, reverse telnet, RSH, SSH, SCP, DLSw, protocol translation, and HTTP sessions that are already established with the device will continue to function properly.

In Cisco IOS, telnet, reverse telnet, RSH, SSH, SCP, DLSw, protocol translation and some HTTP sessions are handled by a virtual terminal (VTY). Each telnet, reverse telnet, RSH, SSH and SCP, DLSw and protocol translation session consumes a VTY. After successful exploitation, the Cisco device can no longer accept any subsequent VTY connections.

Though it is not possible to establish new telnet, reverse telnet, RSH, SSH, SCP, DLSw, protocol translation or HTTP connections to the device after a successful exploitation, the device is only vulnerable on TCP port 23 and the reverse telnet ports listed above.

A successful exploitation of this vulnerability requires a complete 3-way TCP handshake, which makes it very difficult to spoof the source IP address.

Only remote access services that use VTYs are affected. This includes telnet, reverse telnet, RSH, SSH, SCP, DLSw, protocol translation and version 1.0 of the HTTP server. Other device services including, but not limited to, routing protocols, TACACS/RADIUS, Voice over IP (VoIP) and packet forwarding (excluding DLSw and protocol translation) are not affected.

This vulnerability is addressed by Cisco bug ID:

- [CSCef46191](#) ([registered](#) customers only)

Impact

Exploitation of this vulnerability may result in the denial of new telnet, reverse telnet, RSH, SSH, SCP,

DLSw, protocol translation and HTTP connections to a device running IOS. Other access to the device via the console or SNMP is not affected. The device will remain in this state until the problematic TCP connection is cleared, or the device is reloaded (which will clear the problematic session). If no other access methods are available, exploitation of this vulnerability could deny remote access to the device.

Depending on your network architecture, workarounds may be available to mitigate this vulnerability. See below for fixed software that repairs this vulnerability.

Software Versions and Fixes

Cisco is providing fixes for this vulnerability in all currently maintained IOS releases. No software upgrade is required in order to mitigate this vulnerability. See the information below regarding the available configuration workarounds. The software fixes are appearing in regularly scheduled maintenance releases of IOS software.

As more fixed software becomes available, Cisco will update this section of the advisory.

To determine the software running on a Cisco product, log in to the device and issue the **show version** command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS®". On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco product running IOS release 12.0(3) with an installed image name of C2500-IS-L:

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

The release train label is "12.0".

The next example shows a product running IOS release 12.0(2a)T1 with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS Banners is available at <http://www.cisco.com/warp/public/620/1.html#3>.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label). When selecting a release, keep in mind the following definitions:

Maintenance: Most heavily tested, stable, and highly recommended release of a release train in any given row of the table.

Rebuild: Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to repair the vulnerability.

In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco TAC for assistance as shown in the [Obtaining Fixed Software](#) section below.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

The fixes will be available at the Software Center located at <http://www.cisco.com/tacpage/sw-center/>.

For software installation and upgrade procedures, see http://www.cisco.com/en/US/products/ps6350/tsd_products_support_install_and_upgrade.html.

For a current view of all posted and repaired images for Cisco IOS, please check the listing available to registered Cisco.com users at: <http://www.cisco.com/tacpage/sw-center/sw-ios.shtml>.

Major Release	Availability of Repaired Releases*	
Affected 12.0–Based Release	Rebuild	Maintenance
12.0	12.0(5)WC11 Available on 2005–Jan–24	
12.0S	12.0(26)S5	
	12.0(27)S4	
	12.0(28)S2	
		12.0(30)S
Affected 12.1–Based Release	Rebuild	Maintenance
12.1		12.1(26)
12.1E	12.1(20)E5	
	12.1(22)E3	
	12.1(23)E1	
		12.1(26)E Available on 2005–Jan–31
12.1EA	12.1(22)EA2	
Affected 12.2–Based Release	Rebuild	Maintenance
12.2		12.2(27)
12.2BC	12.2(15)BC1f	
	12.2(15)BC2e	
12.2EW	12.2(18)EW2	

12.2JK	12.2(15)JK2	
12.2S	12.2(14)S12	
	12.2(18)S6	
	12.2(20)S6	
	12.2(25)S1	
12.2SE	12.2(20)SE3	
		12.2(25)SE
12.2SU	12.2(14)SU2	
12.2SV		12.2(24)SV
12.2SXB	12.2(17d)SXB5	
12.2SXD	12.2(18)SXD1	
12.2T	12.2(13)T14	
12.2XR	12.2(15)XR2	
Affected 12.3–Based Release	Rebuild	Maintenance
12.3	12.3(6d)	
	12.3(9c)	
	12.3(10a)	
	12.3(12)	
12.3BC	12.3(5a)B2	
		12.3(9a)BC
12.3JA		12.3(2)JA
12.3T	12.3(2)T8	
	12.3(4)T8	
	12.3(7)T4	
	12.3(8)T4	
		12.3(11)T
12.3XD	12.3(4)XD4 Release date not yet determined	
12.3XG	12.3(4)XG2	
12.3XI	12.3(7)XI2	
12.3XK	12.3(4)XK1	
12.3XR	12.3(7)XR3	
12.3XU	12.3(8)XU2	
12.3YD		12.3(8)YD
* All dates are estimated and subject to change.		

Workarounds

The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed.

Mitigation Strategies

Not all of the mitigation strategies listed will work for all customers. Some of the workarounds listed are dependent on which versions and feature-sets of IOS you have in your network.

Enabling SSH and disabling telnet

Note: SSH support is only available in certain IOS feature sets and platforms

Cisco devices that support SSH can enable it by following the steps listed here:

http://cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfssh.html#wp1001167

To disable telnet access to the device, configure the following on all your VTY lines:

```
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
```

Note: Even if SSH is enabled, the IOS device is not protected until telnet access is disabled.

Configuring a VTY Access Class

Note: Cisco Catalyst switch platforms that contain any version of the Route Switch Module (RSM), Route Switch Feature Card (RSFC), Multilayer Switch Module (MSM) or Multilayer Switch Feature Card (MSFC) are able to connect to these modules from the switch Supervisor module using the 'session' command. Although the 'session' command uses telnet internally to connect to the MSM/MSFC, it is not restricted by VTY ACLs.

It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet and SSH.

For more information on restricting traffic to VTYS, please consult:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml

The following example permits access to VTYS from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit host 172.16.1.2
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```

For devices acting as a terminal server, to apply the access class to reverse telnet ports, the access-list must be configured for the aux port and terminal lines as well:

```
Router(config)# line 1 <x>
Router(config-line)# access-class 1 in
```

Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

Configuring Access Lists (ACLs)

In addition to configuring a VTY Access Class, it may be desirable to block all telnet and reverse telnet traffic destined to your network infrastructure.

Telnet and reverse telnet should be blocked as part of a Transit ACL controlling all access to the trusted network. Transit ACLs are considered a network security best practice and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled "Transit Access Control Lists: Filtering at Your Edge" presents guidelines and recommended deployment techniques for transit ACLs:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

Configuring Infrastructure Access Lists (iACLs)

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Configuring Receive Access Lists (rACLs)

For distributed platforms, rACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 series GSR and 12.0(24)S for the 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml

Clearing Hung TCP Connections Using the IOS CLI

The **who** command will show VTY connections to the device:

```
Router# who
  Line      User      Host(s)      Idle      Location
  0 con 0
  * 2 vty 0      idle        00:00:00   192.168.10.72
  3 vty 1      idle        00:00:04   192.168.10.10
```

The above shows two connections on VTYS, one from 192.168.10.72, and one from 192.168.10.10. The * indicates which VTY belongs to the current session. In the above example, the user issuing the who command was connecting from 192.168.10.72. To clear the session from 192.168.10.10, which is on VTY 1, the following command is used:

```
Router# clear tcp line vty 1
```

[confirm]
[OK]

Note: If you are using telnet to connect to the device, accidentally clearing your TCP connection will disconnect your telnet session. If the IOS device has been exploited, it will not be possible to reconnect via telnet. Console access or a device reload will be required to restore service.

Clearing Hung TCP Connections Using SNMP

It is also possible to detect and clear hung TCP connections using SNMP. To detect a hung connection, an SNMP read-only community string must be configured on the device. To reset a connection, an SNMP read-write community string must be configured on the device.

The following document describes, in detail, the process of detecting and clearing hung TCP connections with SNMP:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_problem_troubleshooting09186a00802b93ef.shtml

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who

purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

The Cisco PSIRT is aware of exploitation of this vulnerability and is recommending customers take action to protect themselves.

Status of This Notice: INTERIM

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

Revision 2.4	2004–December–31	Updated availability information for IOS releases. Corrected fixed software version for 12.1E Maintenance release.
Revision 2.3	2004–October–31	Updated table of first fixed releases in the "Software Versions and Fixes" section.
Revision 2.2	2004–October–16	Added information about availability of fixed images to the "Software Versions and Fixes" section.
Revision 2.1	2004–September–09	<p>Changed the title of the Clearing TCP Connections Using the IOS CLI description to Clearing Hung TCP Connections Using the IOS CLI in the Workarounds section.</p> <p>Added the Clearing Hung TCP Connections Using SNMP description to the Workarounds section.</p>
Revision 2.0	2004–September–02	<p>Added DLSw and protocol translation as potentially affected protocols.</p> <p>Explicitly listed affected IOS trains.</p> <p>Added note regarding Catalyst switches to Workarounds section.</p> <p>Added workaround to clear problematic telnet TCP connection via IOS CLI.</p>
Revision 1.3	2004–August–31	<p>Added DLSw as a potentially affected protocol. Explicitly listed affected IOS trains.</p> <p>Added note regarding Catalyst switches to Workarounds section.</p>
Revision 1.2	2004–August–27	Updated the Vulnerable Products section.

		Updated the Configuring a VTY Access Class description in the Workarounds section.
Revision 1.1	2004–August–27	Added the second paragraph to the Details section. Changed the Configuring a VTY Access Class and the Configuring Access Lists (ACLs) descriptions in the Workarounds section.
Revision 1.0	2004–August–27	Initial public release.

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Dec 31, 2004

Document ID: 61671
