

[NEWS] Cisco Telnet DoS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0090.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/29/04

To: list@securiteam.com

Date: 29 Aug 2004 09:31:53 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Cisco Telnet DoS Vulnerability

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. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

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

DETAILS

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

Securiteam: [NEWS] Cisco Telnet DoS Vulnerability

the

<<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml#software>> Software Versions and Fixes section should be considered vulnerable.

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.

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.

Reverse telnet is a feature that allows you to telnet to a Cisco device and then connects to a third device through an asynchronous serial connection. For more information on reverse telnet, consult the following documents:

<http://cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800871ec.html>
http://cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800871ec.html

<http://cisco.com/en/US/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a00800d9bd8.html>
http://cisco.com/en/US/products/sw/iosswrel/ps1826/products_configuration_guide_chapter09186a00800d9bd8.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), and in some cases HTTP (TCP port 80) connections to the device experiencing exploitation will be unsuccessful. Any telnet, reverse telnet, RSH, SSH, SCP and HTTP sessions that are already established with the device will continue to function properly.

In Cisco IOS, telnet, reverse telnet, RSH, SSH, SCP and some HTTP sessions are handled by a virtual terminal (VTY). Each telnet, reverse telnet, RSH,

Securiteam: [NEWS] Cisco Telnet DoS Vulnerability

SSH and SCP 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 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 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 are not affected.

This vulnerability is addressed by Cisco bug ID:

*

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCef46191>>
CSCef46191 (registered customers only)

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/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterprise0900aecd800a4e15.html>
http://www.cisco.com/en/US/products/sw/iosswrel/ios_abcs_ios_networking_the_enterprise0900aecd800a4e15.html.

Securiteam: [NEWS] Cisco Telnet DoS Vulnerability

Impact:

Exploitation of this vulnerability may result in the denial of new telnet, reverse telnet, RSH, SSH, SCP 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. Software will be available to repair this vulnerability.

Software Versions and Fixes:

Cisco is working to release 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 will appear in regularly scheduled maintenance releases of IOS software.

As fixed software becomes available for public release, Cisco will update this

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml#software> section of the advisory.

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.

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

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

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

Securiteam: [NEWS] Cisco Telnet DoS Vulnerability

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.