

[NEWS] Cisco CatOS Telnet Buffer Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0061.html>

From: support@securiteam.com

Date: 02/09/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 9 Feb 2002 12:21:13 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Cisco CatOS Telnet Buffer Vulnerability

SUMMARY

Some Cisco Catalyst switches, running CatOS based software releases, have a vulnerability wherein a buffer overflow in the telnet option handling can cause the telnet daemon to crash and result in a switch reload. This vulnerability can be exploited to initiate a denial of service (DoS) attack.

This vulnerability is documented as Cisco bug ID CSCdw19195. There are workarounds available to mitigate the vulnerability.

DETAILS

Affected products:

Cisco's various Catalyst family of switches run CatOS-based releases or IOS-based releases. IOS-based releases are not vulnerable.

The following Cisco Catalyst Switches are vulnerable:

- * Catalyst 6000 series
- * Catalyst 5000 series
- * Catalyst 4000 series
- * Catalyst 2948G
- * Catalyst 2900

Securiteam: [NEWS] Cisco CatOS Telnet Buffer Vulnerability

Products not affected:

The following Cisco Catalyst switches are not vulnerable:

- * Catalyst 8500 series
- * Catalyst 4800 series
- * Catalyst 4200 series
- * Catalyst 3900 series
- * Catalyst 3550 series
- * Catalyst 3500 XL series
- * Catalyst 4840G
- * Catalyst 4908G-13
- * Catalyst 2948G-13
- * Catalyst 2950
- * Catalyst 2900 XL
- * Catalyst 2900 LRE XL
- * Catalyst 2820
- * Catalyst 1900

No other Cisco product is currently known to be affected by this vulnerability.

Details:

Some Cisco Catalyst switches, running certain CatOS-based software releases, have a vulnerability wherein a buffer overflow in the Telnet option handling can cause the Telnet daemon to crash and result in a switch reload. This vulnerability can be exploited to initiate a denial of service (DoS) attack. Once the switch has reloaded, it is still vulnerable and the attack can be repeated as long as the switch is IP reachable on port 23 and has not been upgraded to a fixed version of CatOS switch software.

This vulnerability is documented as Cisco bug ID CSCdw19195, which requires a CCO account to view and can be viewed after 2002 January 30 at 1500 UTC.

Impact:

This vulnerability can be exploited to produce a denial of service (DoS) attack. When the vulnerability is exploited, it can cause the Cisco Catalyst switch to crash and reload.

Software versions and fixes:

For a table listing all vulnerable versions and their fixes please see:

<http://www.cisco.com/warp/public/707/catos-telrcv-vuln-pub.shtml#Software>
<http://www.cisco.com/warp/public/707/catos-telrcv-vuln-pub.shtml#Software>

Obtaining fixed software:

Cisco is offering free software upgrades to remedy this vulnerability for all affected customers. Customers with service contracts may upgrade to any software release containing the feature sets they have purchased.

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades

Securiteam: [NEWS] Cisco CatOS Telnet Buffer Vulnerability

should be obtained through the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com> <http://www.cisco.com>.

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 assistance with the upgrade, which should be free of charge.

Customers who purchased directly 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

See <http://www.cisco.com/warp/public/687/Directory.shtml> <http://www.cisco.com/warp/public/687/Directory.shtml> for additional TAC contact information, including instructions and e-mail addresses for use in various languages.

Please 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.

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

Workarounds:

The following workarounds can be implemented.

* If the SSH feature is available in the code base, use SSH instead of Telnet and disable Telnet.

For instructions on how to do this, please refer to

http://www.cisco.com/warp/public/707/ssh_cat_switches.html http://www.cisco.com/warp/public/707/ssh_cat_switches.html.

* Apply IP Permit List for Telnet to enable access to the switch's management interface only from the network management workstations.

For instructions on how to do this, please refer to

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_3/config/ip_perm.htm http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_6_3/config/ip_perm.htm.

Please note, this will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface.

Securiteam: [NEWS] Cisco CatOS Telnet Buffer Vulnerability

* On the Catalyst 6000 series switches, if the VLAN Access Control List (ACL) (VACL) feature is available in the code base, you can use VACLs instead of the IP Permit List workaround above.

For instructions on how to do this, please refer to

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/acc_list.htm>
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/acc_list.htm.

Please note, this will not prevent spoofed IP packets with the source IP address set to that of the network management station from reaching the switch's management interface.

* Implement the best practice to assign all of the management interfaces of all the switches in the network to a different VLAN, and apply appropriate ACLs on the router switching between the VLANs.

For an example, see

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/acc_list.htm>
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/acc_list.htm.

* Apply ACLs on routers / switches / firewalls in front of the vulnerable switches such that traffic destined for the Telnet port 23 on the vulnerable switches is only allowed from the network management workstations.

For an example, see

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/acc_list.htm>
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/acc_list.htm.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt-support@cisco.com>>
PSIRT (Product Security Incident Response Team).

=====

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.

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

-
- **Previous message:** support@securiteam.com: "[UNIX] Plumtree Corporate Portal Cross-Site Scripting"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)