

Cisco Security Advisory: Cisco CatOS Telnet Buffer Vulnerability

Document ID: 20776

Advisory ID: cisco-sa-20020129-catos-telrcv

<http://www.cisco.com/warp/public/707/cisco-sa-20020129-catos-telrcv.shtml>

Revision 1.2

Last Updated 2002 February 05 1500 UTC (GMT)

For Public Release 2002 January 29 1500 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: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

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

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20020129-catos-telrcv.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The following Cisco Catalyst Switches are vulnerable:

- Catalyst 6000 series
- Catalyst 5000 series
- Catalyst 4000 series
- Catalyst 2948G, 2980G, 2980G–A, 4912G – use Catalyst 4000 series code base
- Catalyst 2901, 2902, 2926[T,F,GS,GL], 2948 – use Catalyst 5000 series code base

For the switches above, the following CatOS–based switch software revisions are vulnerable.

	Release 4 code base	Release 5 code base	Release 6 code base	Release 7 code base
Catalyst 6000 series	Not applicable	Earlier than 5.5(13)	Earlier than 6.3(4)	Earlier than 7.1(2)
Catalyst 5000 series	Earlier than 4.5(13a)	Earlier than 5.5(13)	Earlier than 6.3(4)	Not applicable
Catalyst 4000 series	All releases	Earlier than 5.5(13)	Earlier than 6.3(4)	Earlier than 7.1(2)

To determine your software revision, type **show version** at the command line prompt.

Products Confirmed Not Vulnerable

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 *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 products are currently known to be affected by these vulnerabilities.

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

This vulnerability has been fixed in the following switch software revisions and the fix will be carried forward in all future releases.

	Release 4 code base	Release 5 code base	Release 6 code base	Release 7 code base
Catalyst 6000 series	Not applicable	5.5(13) and later	6.3(4) and later	7.1(2) and later
Catalyst 5000 series	4.5(13a)	5.5(13) and later	6.3(4) and later	Not applicable
Catalyst 4000 series	Not available	5.5(13) and later	6.3(4) and later	7.1(2) and later

All previous releases must upgrade to the above releases. CatOS switch software release 4.5(13a) for the Catalyst 5000 series is expected on CCO by 2002 February 4. CatOS switch software release 7.1(2) is expected on CCO by 2002 February 6.

Software upgrade can be performed via the console interface. Please refer to software release notes for instructions.

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.
- 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/univered/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.
- 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/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/acc_list.html.

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/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/acc_list.html.

- 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/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/acc_list.html.

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

This vulnerability has been exploited to initiate denial of service (DoS) attacks.

This vulnerability was reported by TESO and is detailed at <http://www.cert.org/advisories/CA-2001-21.html>.

Status of This Notice: FINAL

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.

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 is posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020129-catos-telrev.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
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's Worldwide Web site, 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 1.2	2002-Feb-05	Minor Updates
Revision 1.1	2002-Jan-30	More Workarounds Added
Revision 1.0	2002-Jan-29	For Public Release 2002 January 29 at 1500 UTC

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/go/psirt>. This includes instructions for press inquiries regarding Cisco security notices.

[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: Feb 05, 2002

Document ID: 20776
