

Cisco Security Advisory: Cisco Catalyst Memory Leak Vulnerability

Document ID: 13618

Advisory ID: cisco-sa-20001206-catalyst-memleak

<http://www.cisco.com/warp/public/707/cisco-sa-20001206-catalyst-memleak.s>

Revision 1.3

Last Updated 2000 December 20 0800 UTC (GMT)

For Public Release 2000 December 06 1600 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

A series of failed telnet authentication attempts to the switch can cause the Catalyst Switch to fail to pass traffic or accept management connections until the system is rebooted or a power cycle is performed. All types of telnet authentication are affected, including Kerberized telnet, and AAA authentication.

This vulnerability has been assigned Cisco bug ID **CSCds66191**.

The complete advisory can be viewed at
<http://www.cisco.com/warp/public/707/cisco-sa-20001206-catalyst-memleak.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

These products are vulnerable:

- Catalyst 4000 and 5000 images running version 4.5(2) up to 5.5(4) and 5.5(4a).
- Catalyst 6000 images running version 5.3(1)CSX, up to and including 5.5(4) and 5.5(4a).
- Versions 6.1(1)b and 6.1(2) were not affected in tests for the vulnerability; however, the code fixes were included in those releases as a precautionary measure.
- The Catalyst 5000 series images are installed on the Catalyst 2901, 2902, 2926T, 2926F, 2926GL, 2926GS fixed configuration chassis, and the 5000, 5002, 5500, 5505, and 5509 modular chassis switches.
- The Catalyst 4000 series is installed on the Catalyst 2948G, 2980G, 4003, 4006, and 4912G switches.
- The Catalyst 6000 series is installed on the Catalyst 6009, 6006, 6509, 6509-NEB, and 6506 modular chassis switches.
- The Catalyst 2900XL platform is NOT affected by this vulnerability.

Products Confirmed Not Vulnerable

No other releases of Cisco Catalyst software are affected by this vulnerability. No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The telnet process fails to release resources upon a failed authentication, or a successful login of extremely short duration such as a telnet from within an automated script. This memory leak eventually results in the failure of the switch to perform any other processes, such as forwarding traffic or management; a power cycle or reboot is required for recovery.

The command "**show process memory**" will indicate increased "Holding" memory after failed telnet authentication attempts. This value will not decrease over time except when a reboot, reload, or power cycle occurs. This bug may be triggered over a period of time in the course of normal operation by legitimate users that occasionally fail authentication.

```
lt-6509-e> (enable) sh proc mem

Memory Used:?? 3974544
?????? Free:? 15265168
?????? Total:? 19239712

PID???????? TTY???????? Allocated? Freed?????? Holding??? Process
-----
1?????????? -2?????????? 1707632???? 3488???????? 1704144???? Kernel and Idle

24?????????? -2?????????? 16?????????? 0???????????? 16?????????? telnetd????????
```

Version 4.5(x) of the Catalyst software does not include the command "**show process memory**", so you can use the command "**show mbuf total**" to monitor the memory on the switch. If the "free mbufs" entry decreases and stays low, this indicates a memory leak, which may or may not be related to telnet authentication failures. The Technical Assistance Center can further troubleshoot the device to determine the source of the memory leak if necessary.

Sample Output:

```
switch> (enable) show mbuf total
```

Cisco Security Advisory: Cisco Catalyst Memory Leak Vulnerability

```
mbufs          10296  clusters      5280
free mbufs     9756   clfree        4767
lowest free mbufs 4976  lowest clfree 0
switch> (enable)
```

Impact

This vulnerability enables a Denial of Service attack on the Catalyst switch.

Software Versions and Fixes

Cisco has made the following fixed software available to customers:

- Catalyst Release 4.5(10) for Catalyst 4000 and 5000.
- Catalyst Release 5.5(4b) for Catalyst 4000, 5000 and 6000.
- Catalyst Release 6.1(1)b and 6.1(2) for Catalyst 6000.

The fix will be carried forward into all future releases.

Workarounds

There is no configuration workaround to eliminate the problem. However, if you are unable to upgrade to an unaffected version, you may use other devices to strictly control or prohibit telnet access to the switch, permitting only connections from your local network.

Access control lists on the switch can limit the remote exploitation of the vulnerability. To limit access to known hosts use the following commands:

- **set ip permit enable telnet**
- **set ip permit <addr> [mask]**

Remote management of the switch can also be disabled.

The above workarounds are provided as an option; however, the recommendation is to upgrade to fixed code as soon as possible.

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

Cisco Systems knows of no public discussion nor active exploits involving this vulnerability, which was reported by a customer who noted the memory leak.

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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20001206-catalyst-memleak.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
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- Various internal Cisco mailing lists

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

Revision History

Revision 1.3	2000-December-20	Updated Affected Products list.
Revision 1.2	2000-December-11	Added details of the "show mbuf total" command, which can be used to monitor memory on the switch in the Details section.
Revision 1.1	2000-December-07	Added information about Catalyst software versions 6.1(1)b and 6.1(2) in the Affected Products and Software Versions and Fixes sections.
Revision 1.0	2000-December-06	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 Web site at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices.

All contents are Copyright © 2006-2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Dec 20, 2000

Document ID: 13618

Cisco Security Advisory: Cisco Catalyst Memory Leak Vulnerability

