

Cisco Security Advisory: Cisco Content Services Switch Vulnerability

Document ID: 13613

Advisory ID: cisco-sa-20010131-arrowpoint-cli-fs

<http://www.cisco.com/warp/public/707/cisco-sa-20010131-arrowpoint-cli-fs.s>

Revision 1.2

Last Updated 2001 April 13 1400 UTC (GMT)

For Public Release 2001 January 31 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

The Cisco Content Services (CSS) switch product, also known as Arrowpoint, has two security vulnerabilities once access to the command line interface (CLI) is granted. The first vulnerability, the switch can be forced into a temporary denial of service by an unprivileged user, this is documented in Cisco Bug ID CSCdt08730. The second issue allows a non-privileged user to view filenames and file contents. This is documented in Cisco Bug ID CSCdt12748.

The full text of this advisory can be viewed at:

<http://www.cisco.com/warp/public/707/cisco-sa-20010131-arrowpoint-cli-fs.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The Cisco Content Services Switch is affected by this group of vulnerabilities. The CSS switch is also known as Arrowpoint product, and runs the Cisco WebNS Software.

Cisco CSS 11050, CSS 11150, and CSS 11800 hardware platforms are affected by this group of vulnerabilities.

No other Cisco products are affected by this group of vulnerabilities.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The Cisco CSS11000 must be configured to permit command line access to users by providing a management address and defining user accounts. Once command line access is gained by non privileged users (defined user accounts without administrative privileges), running a command requiring a filename, and providing a filename that is the maximum length of the input buffer can cause the switch to reboot, and a system check to be started which will prevent normal function of the switch for up to 5 minutes. The **show script**, **clear script**, **show archive**, **clear archive**, **show log**, and **clear log** commands are capable of causing the CSS to restart if the specified file name is the maximum length of the input buffer. Cisco Bug ID CSCdt08730.

If command line access is not restricted, a non privileged user (defined user account without administrative privileges) can gain information on the directory structure by requesting non-existent filenames. Additionally, the non privileged user can gain read access for files if the directory structure of the target files are known to the user. Cisco Bug ID CSCdt12748 describes this file system vulnerability.

Impact

The vulnerability described in CSCdt08730 can be continuously reproduced to produce a Denial of Service attack. The additional vulnerabilities provide unauthorized access to important files such as the configuration files, and directory structure information. If access to the command line interface is well protected and restricted, then these vulnerabilities are minimized.

Software Versions and Fixes

CSCdt08730 is resolved in revision 4.01(12s), and revision 3.10 (71s) of Cisco WebNS software. The file system information disclosure vulnerabilities are resolved in revision 4.01(23s) and revision 4.10(13s).

Workarounds

Access control lists can be applied to restrict access to the Cisco CSS device, as well as additional firewall or access lists to restrict connection to the management interface. Access control lists also affect traffic to the Virtual interface of the Cisco CSS device, so must be applied with care. For further details on configuring access lists please refer to the product documentation:

<http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/bsscfdgd/profiles.htm>

<http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/advcfggd/sgacleql.htm>

Additionally, the use of SSH to prevent snooping of the management traffic to the device is encouraged.

Telnet service can also be disabled, for many customers in a co-location environment this is not a feasible option, but is included in this section for customers that may have the ability to implement this configuration.

```
CS150(config)# telnet access disabled
```

Additionally, it is recommended to select strong passwords in accordance with your own security policies, and to adhere to your own security policies on changing passwords frequently, or when staffing changes occur.

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 not aware of any public announcements or malicious use of the vulnerabilities described in this advisory. These vulnerabilities were discovered by a Security Consulting firm during a customer security audit.

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-20010131-arrowpoint-cli-fs.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 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

	2001-April-13	
--	---------------	--

Revision
1.2

The Software Versions and Fixes section was changed from :
"CSCdt08730 is resolved in revision 4.01(12s), and revision 3.10 (71s) of Cisco WebNS software. The file system information disclosure vulnerabilities are scheduled to be fixed, but are currently unresolved. Workarounds are recommended in the interim. This notice will be updated when the vulnerabilities are resolved, or monthly until the vulnerabilities are resolved."

to:

"CSCdt08730 is resolved in revision 4.01(12s), and revision 3.10 (71s) of Cisco WebNS software. The file system information disclosure vulnerabilities are resolved in revision 4.01(23s) and revision 4.10(13s)."

The status of this notice was changed from INTERIM to FINAL, and the wording under the Status of This Notice section was changed from: "This is an interim notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of our ability. Cisco anticipates issuing updated versions of this notice as the software is updated. Cisco will update this notice by 2001-MAR-01."

to:

"This is an final notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this notice

		unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this notice."
Revision 1.1	2001-February-02	<p>The following sentence was changed: "The Cisco Content Services (CSS) switch product, also known as Arrowpoint, has several security vulnerabilities once access to the command line interface (CLI) is granted."</p> <p>to:</p> <p>"The Cisco Content Services (CSS) switch product, also known as Arrowpoint, has two security vulnerabilities once access to the command line interface (CLI) is granted."</p> <p>The word "several" was changed to "two"</p>
Revision 1.0	2001-January-31	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>.

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

Updated: Apr 13, 2001

Document ID: 13613
