

[NEWS] Content Service Switch Web Management HTTP Processing Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0075.html>

From: support@securiteam.com

Date: 05/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 18 May 2002 22:47:21 +0200 (CEST)

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.

Content Service Switch Web Management HTTP Processing Vulnerabilities

SUMMARY

The Cisco Content Service Switch (CSS) 11000 series switches are susceptible to a soft reset caused by improper handling of HTTP POST requests to the web management interface.

These vulnerabilities are documented as Cisco bug ID's CSCdx41911 and CSCdw26696.

DETAILS

Affected Products:

The CSS 11000 series switches (formerly known as Arrowpoint), consist of the CSS 11050, CSS 11150 and CSS 11800 hardware platforms. They run the Cisco WebNS Software.

All CSS 11000 series switches running the following WebNS software revisions are affected by these vulnerabilities.

- * 04.01.053s and earlier
- * 05.00.038s and earlier
- * 05.01.012s and earlier

Securiteam: [NEWS] Content Service Switch Web Management HTTP Processing Vulnerabilities

* 05.02.005s and earlier

The CSS 11500 Series switches running the following WebNS software revisions are affected by these vulnerabilities:

* 05.10.0.01

No other Cisco product is currently known to be affected by these vulnerabilities.

To determine your software revision, type version at the command line prompt on your Content Service Switch.

Details:

CSCdw26696

The CSS formerly used TCP port 8081 for its web management interface. The web server that listens on port 8081 did not understand XML data and in trying to process the incoming request would result in a soft reset of the device. Currently all web management interface traffic should be directed over SSL or "https".

CSCdx41911

The CSS may be forced to reboot by sending an HTTPS post request to the web management interface of the device. This may occur even if the sender of the request is not yet authenticated to the device.

Impact:

Both defects may reboot the device resulting in a Denial of Service (DoS) due to decreased availability.

Software Versions and Fixes:

Cisco WebNS Software

Version Affected – Fixed Regular Release. Fix carries forward into all later versions.

4.01 – 5.00.045 (available 2002/06/04)

5.0 – 5.00.045 (available 2002/06/04)

5.01 – 5.03

5.02 – 5.03

5.10 – TBD

Obtaining Fixed Software:

Cisco is offering free software upgrades to address this vulnerability for all affected customers. Customers may only install and expect support for the feature sets they have purchased.

Customers with service contracts should contact their regular update channels to obtain any software release containing the feature sets they have purchased. For most customers with service contracts, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Web site at <<http://www.cisco.com>> <http://www.cisco.com>.

Securiteam: [NEWS] Content Service Switch Web Management HTTP Processing Vulnerabilities

Customers whose Cisco products are provided or maintained through a 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 obtaining the free software upgrade(s).

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 obtain fixed software by contacting the Cisco Technical Assistance Center (TAC) using the contact information listed below. In these cases, customers are entitled to obtain an upgrade to a later version of the same release or as indicated by the applicable row in the Software Versions and Fixes table (noted above).

Cisco 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/DirTAC.shtml>> <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.

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade.

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

Workarounds:

- * Disable web-based management of the device:
restrict web-mgmt
restrict xml

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@cisco.com>> Cisco Systems 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: "[NEWS] Transparent Cache Engine and Content Engine TCP Relay Vulnerability"
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)