

# Cisco Security Advisory: Content Service Switch Web Management HTTP Processing Vulnerabilities

Document ID: 23667

Advisory ID: cisco-sa-20020515-css-http-post

<http://www.cisco.com/warp/public/707/cisco-sa-20020515-css-http-post.shtml>

## Revision 1.3

Last Updated 2002 May 28 1200 UTC (GMT)

For Public Release 2002 May 15 1800 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: INTERIM](#)  
[Distribution](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## 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.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20020515-css-http-post.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable 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
- 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

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

## Products Confirmed Not Vulnerable

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

## 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 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

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your

contracted maintenance provider for assistance.

#### Version Affected

Fixed Regular Release. Fix carries forward into all later versions.

4.01

5.00.045 (available 2002/06/11)

5.0

5.00.045 (available 2002/06/11)

5.01

5.03

5.02

5.03

5.10

TBD

## Workarounds

Disable web-based management of the device:

```
restrict web-mgmt
```

```
restrict xml
```

## 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](mailto: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 vulnerability described by CSCdx41911 was originally reported to Cisco by James Mancini of Netreo Inc. The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

## Status of This Notice: INTERIM

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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-20020515-css-http-post.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- 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

Revision 1.3	2002-May-18	Updated availability dates for fixed software releases.
Revision 1.2	2002-May-17	Updated availability dates for fixed software releases.
Revision 1.1	2002-May-16	Updated title of document to more accurately reflect the problem.
Revision 1.0	2002-May-15	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](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: May 28, 2002

Document ID: 23667

---