

# Cisco Security Advisory: Cisco Content Service Switch 11000 Series FTP Vulnerability

Document ID: 13614

Advisory ID: cisco-sa-20010517-arrowpoint-ftp

<http://www.cisco.com/warp/public/707/cisco-sa-20010517-arrowpoint-ftp.shtml>

## Revision 1.0

For Public Release 2001 May 17 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

The Cisco Content Service Switch (CSS) 11000 series switches do not enforce the correct restrictions for a non privileged user opening an FTP connection to them. All users with valid accounts can use the GET and PUT commands to read and write any file on the system. This vulnerability results in users gaining access to secure data.

This vulnerability is documented as Cisco bug ID CSCdt64682.

This advisory will be posted at  
<http://www.cisco.com/warp/public/707/cisco-sa-20010517-arrowpoint-ftp.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 switches running the following WebNS software revisions are affected by this vulnerability

- earlier than 4.01B23s
- earlier than 4.10B13s

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

## Products Confirmed Not Vulnerable

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

## Details

A non privileged user (user account without administrative privileges) can open an FTP connection to a CSS 11000 series switch and use GET and PUT FTP commands, with no user level restrictions enforced.

This vulnerability is documented as Cisco bug ID CSCdt64682, which requires a CCO account to view.

## Impact

A non privileged user can gain access to files on the switch they normally would not have access to. This vulnerability can be minimized by restricting ftp access to the CSS 11000 series switch.

## Software Versions and Fixes

This vulnerability has been fixed in the following Cisco WebNS software revisions

- 4.01B23s or later
- 4.10B13s or later

## Workarounds

Don't configure non-privileged users on the switch. ( None are created by default. )

Use the restrict command to enable or disable FTP access to the CSS. (FTP access is enabled by default.)  
(config)# restrict ftp Access control lists can be applied to restrict FTP access to the Cisco CSS device.

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/bsscfcgd/profiles.htm>

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

## 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 Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

This vulnerability was reported to Cisco by a Cisco customer.

## 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-20010517-arrowpoint-ftp.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)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [comp.dcom.sys.cisco](mailto: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

Revision 1.0	2001 May 17	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 17, 2001

Document ID: 13614

---