

Cisco Security Advisory: Cisco Content Service Switch 11000 Series Web Management Vulnerability

Document ID: 10931

Advisory ID: cisco-sa-20010531-arrowpoint-webmgmt

<http://www.cisco.com/warp/public/707/cisco-sa-20010531-arrowpoint-webmgmt>

Revision 3.0

Last Updated 2003 April 18 1500 UTC (GMT)

For Public Release 2001 May 31 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 accessing the web management URL.

After successful authentication users are redirected to the web management URL. If users directly connect to the redirected URL they are granted access to the web management interface without having to reauthenticate. This vulnerability results in users gaining access to secure data.

This vulnerability is documented as Cisco bug IDs CSCdu20931 and CSCdw08549.

This advisory will be posted at
<http://www.cisco.com/warp/public/707/cisco-sa-20010531-arrowpoint-webmgmt.shtml>.

This advisory is being re-released because the vulnerability was not completely fixed previously. Users are still vulnerable and should apply the workarounds in the Workarounds section to mitigate the affects of the

vulnerability.

Affected Products

This section supplies 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 *any* WebNS software revision are affected by this vulnerability.

Products Confirmed Not Vulnerable

No other Cisco product is currently known to be affected by this vulnerability.

Details

If users bookmark the URL they are redirected to after a successful authentication on the CSS 11000 series switches, they can later access the web management interface without having to reauthenticate.

This advisory is being re-released because the vulnerability was not completely fixed previously. Users are still vulnerable and should apply the workarounds in the Workarounds section to mitigate the affects of the vulnerability.

This vulnerability is documented as Cisco bug IDs CSCdu20931 and CSCdw08549, which require a CCO account to view.

Impact

A user can gain access to the web management interface without being authenticated on the CSS 11000 series switch. This vulnerability can be minimized by restricting http access to the CSS 11000 series switch.

Software Versions and Fixes

This vulnerability is fixed in the Cisco WebNS software version 6.10 which will be available for download by the end of May 2003.

Workarounds

Web Management can be disabled on the switch.

Access control lists can be applied to restrict HTTP access to the Cisco CSS 11000 series switch. Access control lists also affect traffic to the Virtual interface of the Cisco CSS 11000 series switch, so must be applied with care. For further details on configuring access lists, please refer to the product documentation:

http://www.cisco.com/en/US/products/hw/contnetw/ps789/products_configuration_guide_chapter09186a00800d6b2d.1

Obtaining Fixed Software

Cisco will be offering free software upgrades to remedy this vulnerability for all affected customers. Customers with service contracts may upgrade to any software release containing the feature sets they have purchased.

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 assistance with the upgrade, which should be free of charge.

Customers without Service Contracts

Customers without contracts should get their upgrades by contacting the Cisco Technical Assistance Center (TAC).

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

See <http://www.cisco.com/warp/public/687/Directory.shtml> for additional TAC contact information, including instructions and e-mail addresses for use in various languages.

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

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

Exploitation and Public Announcements

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

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 is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20010531-arrowpoint-webmgmt.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
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- 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

3.0	2003-April-18	Updated availability estimate and specific version of repaired code.
2.0	2002-August-14	Revised interim public release.
1.0	2001-May-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.

Cisco Security Advisory: Cisco Content Service Switch 11000 Series Web Management Vulnerability

