

Table of Contents

<u>Cisco Security Advisory: Cisco CSS 11000 Series Content Services Switches Malformed UDP Packet Vulnerability</u>	1
<u>Document ID: 49584</u>	1
<u>Revision 1.2</u>	1
<u>Last Updated 2005 February 2 at 1800 UTC (GMT)</u>	1
<u>For Public Release 2004 March 4 at 1700 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	1
<u>Details</u>	2
<u>Impact</u>	2
<u>Software Versions and Fixes</u>	2
<u>Obtaining Fixed Software</u>	3
<u>Workarounds</u>	3
<u>Exploitation and Public Announcements</u>	4
<u>Status of This Notice: FINAL</u>	4
<u>Distribution</u>	4
<u>Revision History</u>	4
<u>Cisco Security Procedures</u>	5

Cisco Security Advisory: Cisco CSS 11000 Series Content Services Switches Malformed UDP Packet Vulnerability

Document ID: 49584

Revision 1.2

Last Updated 2005 February 2 at 1800 UTC (GMT)

For Public Release 2004 March 4 at 1700 UTC (GMT)

Please provide your feedback on this document.

[Summary](#)
[Affected Products](#)
[Details](#)
[Impact](#)
[Software Versions and Fixes](#)
[Obtaining Fixed Software](#)
[Workarounds](#)
[Exploitation and Public Announcements](#)
[Status of This Notice: FINAL](#)
[Distribution](#)
[Revision History](#)
[Cisco Security Procedures](#)

Summary

The CSS 11000 Series Content Services Switches are vulnerable to a Denial of Service (DoS) attack caused by malformed UDP packets received over the management port.

This vulnerability is documented as Cisco bug ID CSCed45747. There is no workaround available to mitigate the effects of this vulnerability. Cisco is providing fixed software, and customers are recommended to upgrade to it.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20040304-css.shtml>.

Affected Products

The CSS 11000 Series Content Services Switches (formerly known as Arrowpoint) consist of the CSS 11050, CSS 11100, CSS 11150, and CSS 11800 hardware platforms. They run the Cisco WebNS software.

WebNS Release Train	Affected Releases
5.0(x)	earlier than 05.0(04.07)S

6.10(x)	earlier than 06.10(02.05)S
---------	---------------------------------------

For clarification, the CSS 11500 Series Content Services Switches consisting of 11501, 11503, and 11506 , the Cisco Global Site Selector (GSS) series switches, and the Content Switching Module (CSM) are not affected by this vulnerability.

No other Cisco products are currently known to be affected by this vulnerability.

To determine your hardware model and software revision, type **show chassis** at the command line prompt.

Details

If malformed UDP packets are sent to UDP port 5002, the default port for **app-udp**, on the management port of the CSS 11000 Series Content Services Switch running Cisco WebNS release 5.0(x) and 6.10(x) release trains the switch may reload. This vulnerability exists even when the Network Proximity feature is not configured on the CSS 11000 Series Content Services Switch. Please refer to http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/css_610/advcggd/proximty.htm for more details on the Network Proximity feature.

Access to the management port of the CSS 11000 Series Content Services Switches is available solely through the physical management interface on the device; access via circuit VLANs is not implemented, and therefore the vulnerability can only be exploited through the management port.

This vulnerability is documented in the Cisco Bug Toolkit (registered customers only) as Bug ID CSCed45747. Cisco WebNS release 7.10(x), 7.20(x), and 7.30(x) release trains have also had code changes but due to architectural differences they are not affected by this vulnerability.

The Internetworking Terms and Cisco Systems Acronyms online guides can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/>.

Impact

Exploitation of this vulnerability results in a reload of the CSS 11000 Series Content Services Switches. Repeated exploitation of the vulnerability may result in a Denial of Service (DoS) for the CSS 11000 Series Content Services Switches.

Software Versions and Fixes

WebNS Release Train	Fixed Releases
5.0(x)	05.0(04.07)S and later
6.10(x)	06.10(02.05)S and later

The procedure to upgrade to a fixed software version is available under "Upgrading Your CSS Software" in the CSS Administration Guide (for version 6.x), or "Upgrading Your CSS Software" in the CSS Basic Configuration Guide (for version 5.x). The steps can be accessed online at http://www.cisco.com/univercd/cc/td/doc/product/webscale/css/css_610/admgd/upgrade.htm.

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. 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 the Cisco Connection Online Software Center at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

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/cgi-bin/tablebuild.pl/webns-interim?psrtdcat20e2>. To access the software download URL, you must be a registered user and you must be logged in.

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 software upgrade(s).

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) using the contact information listed below. In these cases, customers are entitled to obtain a free upgrade to a later version of the same release or as indicated by the applicable corrected software version in the Software Versions and Fixes section (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> 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 upgrade. 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.

Workarounds

There is no workaround for this vulnerability. Customers may be able to mitigate the affects of the vulnerability by controlling access to the UDP port 5002 on the management port of the CSS 11000 Series Content Services Switch to allow access only from required network devices or by disallowing access if the Network Proximity feature is not configured.

The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

Exploitation and Public Announcements

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

This vulnerability was reported to Cisco PSIRT by Timothy Arnold.

Status of This Notice: FINAL

This is a final notice. Although Cisco cannot guarantee the accuracy of all statements in this advisory, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this advisory.

A stand-alone copy or paraphrase of the text of this security advisory 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-20040304-css.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key having the fingerprint 8C82 5207 0CA9 ED40 1DD2 EE2A 7B31 A8CF 32B6 B590 and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com

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 1.2	2005 February 2	Fixed broken link to the upgrade procedure document in the Software Versions and Fixes section.
Revision 1.1	2004 March 04	Added CSS 11100 to the affected products section.
Revision 1	2004 March 04	Initial Release.

04

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>.

This advisory is copyright 2004 by Cisco Systems, Inc. This advisory may be redistributed freely after the release date given at the top of the text, provided that redistributed copies are complete and unmodified, including all date and version information.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Feb 02, 2005

Document ID: 49584
