

# [VulnWatch] Cisco Security Advisory: Cisco 11500 Content Services Switch HTTP Request Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-04/msg00002.html>

---

- *From:* Cisco Systems Product Security Incident Response Team <[psirt@xxxxxxxx](mailto:psirt@xxxxxxxx)>
  - *Date:* Wed, 05 Apr 2006 17:00:00 +0200
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Cisco 11500 Content Services Switch HTTP Request Vulnerability

Advisory ID: cisco-sa-20060405-css

<http://www.cisco.com/warp/public/707/cisco-sa-20060405-css.shtml>

Revision 1.0

For Public Release 2006 April 05 1500 GMT (UTC)

-----

Contents

=====

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

=====

# [VulnWatch] Cisco Security Advisory: Cisco 11500 Content Services Switch HTTP Request Vulnerability

Cisco CSS 11500 Series Content Services Switches configured for Hyper Text Transfer Protocol (HTTP) compression are vulnerable to a Denial of Service (DoS) attack when processing valid, but obsolete, or specially crafted HTTP request.

Cisco has made free software available to address this vulnerability for affected customers. The workaround is to disable HTTP compression.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060405-css.shtml>.

## Affected Products

=====

## Vulnerable Products

+-----

Cisco CSS 11500 Series Content Services Switches that are configured for HTTP compression are vulnerable.

A Cisco CSS11500 that is configured for HTTP compression will have configuration similar to the following, which can be seen by issuing the show running-config command:

```
service compression_service_name
....
....
compress enable
....
....
```

## Products Confirmed Not Vulnerable

+-----

Cisco CSS 11500 Series Content Services Switches that are not configured for HTTP compression are not vulnerable.

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

## Details

=====

The Cisco CSS 11500 Content Service Switch is load balancing device designed to provide robust, scalable network services (Layer 4-7) for data centers. The Cisco CSS 11500 performs an analysis of protocol headers and directs requests to an appropriate resource based on configurable policies. With a compression module, a Cisco CSS 11500

## [VulnWatch] Cisco Security Advisory: Cisco 11500 Content Services Switch HTTP Request Vulnerability

can compress HTTP client traffic.

For more information about HTTP compression on CSS 11500 switches, refer to the following URL:

[http://www.cisco.com/en/US/products/hw/contnetw/ps792/products\\_configuration\\_guide\\_chapter09186a0080579fef.h](http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_configuration_guide_chapter09186a0080579fef.h)

A Cisco CSS 11500 enabled for HTTP compression may reload after receiving valid, but obsolete, or specially crafted HTTP request.

Cisco CSS 11500 switches where HTTP compression is not used or is disabled are not affected by this vulnerability.

The vulnerability is documented in the following Cisco Bug ID:

\* CSCek24160 ( registered customers only) CSS cores while using software compression.

### Impact

=====

Successful exploitation of the vulnerability may result in the reload of the device. Repeated exploitation could result in a sustained DoS attack.

### 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.

This issue is fixed in version 8.10.1.6 of CSS software. Fixed software can be downloaded from the following URL::

<http://www.cisco.com/cgi-bin/tablebuild.pl/css11500-maint?psrtdcat20e2>

### Workarounds

=====

The workaround is to disable HTTP compression. That can be accomplished using the compress disable command.

### 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@xxxxxxxx" or "security-alert@xxxxxxxx" 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@xxxxxxxxx

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 vulnerability described in this advisory.

This vulnerability was reported to Cisco by a 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 is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20060405-css.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@xxxxxxxxx
- \* first-teams@xxxxxxxxx
- \* bugtraq@xxxxxxxxxxxxxxxxxxxxx

[VulnWatch] Cisco Security Advisory: Cisco 11500 Content Services Switch HTTP Request Vulnerability

- \* vulnwatch@xxxxxxxxxxxxxx
- \* cisco@xxxxxxxxxxxxxxxxxxx
- \* cisco-nsp@xxxxxxxxxxxxxxxxxxx
- \* full-disclosure@xxxxxxxxxxxxxxxxxxx
- \* comp.dcom.sys.cisco@xxxxxxxxxxxxxxxxxxx

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 | | Initial |
| 1.0 | 2006-April-05 | 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>.

-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.4.2.2 (GNU/Linux)

iD8DBQFEM9VQ8NUAbBmDaxQRArYhAKCoiVAsJn2VMpU1Yq+LFHlpuQjWUACeJnNR  
iQO7/i9S9A1I0dFelyHEZxw=  
=17Fo

-----END PGP SIGNATURE-----