

Cisco Security Advisory: Cisco Content Switching Module Memory Leak Vulnerability

Advisory ID: cisco-sa-20080514-csm

<http://www.cisco.com/warp/public/707/cisco-sa-20080514-csm.shtml>

Revision 1.0

For Public Release 2008 May 14 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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 Switching Module (CSM) and Cisco Content Switching Module with SSL (CSM-S) contain a memory leak vulnerability that can result in a denial of service condition. The vulnerability exists when the CSM or CSM-S is configured for layer 7 load balancing. An attacker can trigger this vulnerability when the CSM or CSM-S processes TCP segments with a specific combination of TCP flags while servers behind the CSM/CSM-S are overloaded and/or fail to accept a TCP connection.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080514-csm.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

The Cisco CSM and Cisco CSM-S are affected by the vulnerability described in this document if they are running an affected software version and are configured for layer 7 load balancing.

The following versions of the Cisco CSM software are affected by this vulnerability: 4.2(3), 4.2(3a), 4.2(4), 4.2(5), 4.2(6), 4.2(7), and 4.2(8).

The following versions of the Cisco CSM-S software are also affected by this vulnerability: 2.1(2), 2.1(3), 2.1(4), 2.1(5), 2.1(6), and 2.1(7).

To determine the software version in use by the CSM or CSM-S, log into the supervisor of the chassis that hosts the CSM or CSM-S modules and issue the command **show module version** (Cisco IOS) or **show version** (Cisco CatOS). CSM modules will display as model "WS-X6066-SLB-APC", CSM-S modules will display as model "WS-X6066-SLB-S-K9", and the software version will be indicated next to the "Sw:" label.

Note that the output from **show module version** (for Cisco IOS) is slightly different from the output from **show version** (for Cisco CatOS). However, in both cases the model names will read as previously described, and the software version will be easily identified by looking for the "Sw:" label.

The following example shows a CSM in slot number 4 running software version 4.2(3):

```

switch>show module version
Mod  Port Model                Serial #    Versions
-----
1    3    WS-SVC-AGM-1-K9            SAD092601W5 Hw : 1.0
                                           Fw : 7.2(1)
                                           Sw : 5.0(3)
2    6    WS-SVC-FWM-1              SAD093200X8 Hw : 3.0
                                           Fw : 7.2(1)
                                           Sw : 3.2(3)1
3    8    WS-SVC-IDSM-2            SAD0932089Z Hw : 5.0
                                           Fw : 7.2(1)
                                           Sw : 5.1(6)E1
4    4    WS-X6066-SLB-APC        SAD093004BD Hw : 1.7
                                           Fw :
                                           Sw : 4.2(3)
5    2    WS-SUP720-3B            SAL0934888E Hw : 4.4
                                           Fw : 8.1(3)
                                           Sw : 12.2(18)

SXF11
                                           Sw1: 8.6

(0.306)R3V15
      WS-SUP720            SAL09348488 Hw : 2.3
                                           Fw : 12.2(17r)

S2
                                           Sw : 12.2(18)

SXF11
      WS-F6K-PFC3B        SAL0934882R Hw : 2.1

```

A Cisco CSM or CSM-S is configured for layer 7 load balancing if one or more layer 7 Server Load Balancing (SLB) policies are referenced in the configuration of a virtual server. There are six possible types of SLB policies: "client-group", "cookie-map", "header-map", "reverse-sticky", "sticky-group", and "url-map". Of these, the "client-group" policy type is always a layer 4 policy. The remaining policy types are layer 7 policies and, if used, would render a device affected by the vulnerability described in this document. The following example shows a CSM module that is configured for layer 7 load balancing. Note the SLB policy "TEST-SPORTS-50", which uses "url-map" and "header-map" layer 7 policies, and that is applied to the virtual server named "WEB":

```

module ContentSwitchingModule 5
[... ]
!
```

```
policy TEST-SPORTS-50
url-map SPORTS
header-map TEST
client-group 50
serverfarm WEBFARM2
!
vserver WEB
virtual 10.20.221.100 tcp www
serverfarm WEBFARM
persistent rebalance
slb-policy TEST-SPORTS-50
inservice
```

☐ Products Confirmed Not Vulnerable

Only Cisco CSM modules running indicated 4.2 versions are affected by this vulnerability. CSM software versions 4.1, 3.2 and 3.1 are not affected by this vulnerability.

Cisco CSM-S modules running indicated 2.1 versions are the only vulnerable versions of software for that product.

Cisco CSM and CSM-S modules that are not configured for layer 7 load balancing are not affected by this vulnerability.

The Cisco IOS SLB feature is not affected by this vulnerability.

No other Cisco products are currently known to be affected by this vulnerability. The Cisco Secure Content Accelerator is not affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

The Cisco CSM is an integrated SLB line card for the Catalyst 6500 and 7600 Series that is designed to enhance the response time for client traffic to end points including servers, caches, firewalls, Secure Sockets Layer (SSL) devices, and VPN termination devices.

The Cisco CSM-S combines high-performance SLB with SSL offload. The CSM-S is similar to the CSM; however, unlike the CSM, the CSM-S can terminate and initiate SSL-encrypted traffic. This ability allows the CSM-S to perform intelligent load balancing while ensuring secure end-to-end encryption.

A memory leak vulnerability exists in some versions of the software for the Cisco CSM and Cisco CSM-S when the CSM or CSM-S is configured for layer 7 load balancing (see the "Vulnerable Products" section for configuration details). The memory leak is triggered when the CSM or CSM-S processes TCP segments with a specific combination of TCP flags and fails to make a load balancing decision because servers behind the CSM/CSM-S are overloaded and/or fail to accept a TCP connection.

The memory leak can be detected by issuing the command **show module ContentSwitchingModule <slot #> tech-support all | include Outstanding** on the supervisor and checking the command output for a high number of outstanding buffers as seen in the following example:

```
switch#show module ContentSwitchingModule 10 tech-support
all | include Outstanding
Outstanding slowpath(low pri) buffers      0
0
Outstanding slowpath(high pri) buffers    0
0
Outstanding blocks                          0
0
Outstanding small buffers                   0
0
Outstanding medium buffers                 823
0
Outstanding large buffers                  0
0
Outstanding sessions                       0
0
Outstanding Closes                         0
0
Close Relinquish Outstanding              0
```

Because small, medium, and large buffers can be affected by the memory leak, administrators are advised to check the number of these buffers in the output from the preceding command to accurately detect a memory leak condition.

This vulnerability is documented in Cisco Bug ID [CSCsl40722](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2008-1749.

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsl40722 - CSM: Potential buffer loss with irregular client streams					
Calculate the environmental score of CSCsl40722					
CVSS Base Score - 7.8					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - 6.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of this vulnerability against a system running a vulnerable version of the Cisco CSM or the Cisco CSM-S software may cause the CSM or CSM-S to stop passing traffic. Repeated attacks may result in a prolonged DoS condition, which could affect the services that are offered by the end point devices behind the CSM or CSM-S.

Note that the supervisor or any other non-CSM or non-CSM-S service module in the same chassis of the Catalyst 6500 switch or 7600 Series router that hosts the CSM or CSM-S will not be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ **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 vulnerability is fixed in version 4.2.9 of the Cisco CSM software, and in version 2.1.8 of the Cisco CSM-S software.

CSM software can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-csm?psrtdcat20e2> ([registered](#) customers only) .

Information on how to upgrade the CSM software is available at http://www.cisco.com/en/US/products/hw/modules/ps2706/products_tech_note09186a0080094526.shtml.

CSM-S software can be downloaded from <http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-csms?psrtdcat20e2> ([registered](#) customers only) .

Information on how to upgrade the CSM-S software is available at http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/csms/2.1.1/configuration/guide/getstart.html#wp1041858.

[Top of the section](#) [Close Section](#)

☐ Workarounds

There are no workarounds for this vulnerability. When the Cisco CSM or Cisco CSM-S has run out of memory it will simply stop passing traffic and it will have to be reloaded. The CSM and CSM-S can be reloaded via the command **hw-module module <CSM or CSM-S slot number> reset** (Cisco IOS) or via the command **reset <CSM or CSM-S slot number>** (Cisco CatOS) from the privileged EXEC prompt of the supervisor. There is no need to reload the supervisor.

[Top of the section](#) [Close Section](#)

☐ Obtaining Fixed Software

Cisco has released free software updates that address this vulnerability. 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/en/US/docs/general/warranty/English/EU1KEN.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of 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 localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **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 discovered during the investigation of customer support cases.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20080514-csm.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
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.0	2008-May-14	Initial public release
--------------	-------------	------------------------

[Top of the section](#) [Close Section](#)

☐ 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>.

[Top of the section](#) [Close Section](#)

Help us help you.



Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor



This document solved my problem.

- Yes
- No
- Just browsing



Suggestions for improvement:

(256 character limit)

[Home](#)[How to Buy](#)[Login](#)[Profile](#)[Feedback](#)[Site Map](#)[Help](#)

