

Cisco Security Advisory: Denial of Service Vulnerabilities in Content Switching Module

Advisory ID: cisco-sa-20070905-csm

<http://www.cisco.com/warp/public/707/cisco-sa-20070905-csm.shtml>

Revision 1.1

Last Updated 2008 April 25 1430 UTC (GMT)

For Public Release 2007 September 5 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 Modules (CSM) and Cisco Content Switching Module with SSL (CSM-S) contain two vulnerabilities that can lead to a denial of service (DoS) condition. The first vulnerability exists when processing TCP packets, and the second vulnerability affects devices with *service termination* enabled.

Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070905-csm.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

These vulnerabilities were identified in CSM software version 4.2 and CSM-S software version 2.1. The following table helps illustrate the vulnerable software versions for these products:

Vulnerability	CSM	CSM-S
TCP packet Processing DOS	4.2 Prior to 4.2.3a	2.1 Prior to 2.1.2a
Service Termination	4.2 Prior to 4.2.7	2.1 Prior to 2.1.6

To determine the software running on a Content Switching Module, log in to the Catalyst switch and issue the show version command.

The following example shows a CSM running software version 4.2(2) in a Supervisor running CatOS. Supervisors running CatOS or IOS will have similar output. The version of the CSM is shown on the module labeled WS-X6066-SLB-APC as illustrated in the following output.

```
Console>show version
WS-C6506 Software, Version NmpSW: 7.6(9)
Copyright (c) 1995-2004 by Cisco Systems
NMP S/W compiled on Aug 27 2004, 20:05:14

System Bootstrap Version: 7.1(1)
System Boot Image File is 'disk0:cat6000-sup2k8.7-6-9.bin'
System Configuration register is 0x2102

Hardware Version: 3.0 Model: WS-C6506 Serial #: TBA05360375

PS1 Module: WS-CAC-1300W Serial #: ACP05061071
PS2 Module: WS-CAC-1300W Serial #: ACP05060407

Mod Port Model Serial # Versions
-----
1 2 WS-X6K-SUP2-2GE SAD055104YY Hw : 3.2
Fw : 7.1(1)
Fw1: 6.1(3)
Sw : 7.6(9)
Sw1: 7.6(9)
WS-F6K-PFC2 SAD055104H5 Hw : 3.0
Sw :
WS-X6K-SUP2-2GE SAD055104YY Hw : 3.2
Sw :
2 48 WS-X6248-RJ-45 SAD0501084U Hw : 1.4
```

Fw : 5.4(2)
Sw : 7.6(9)

5 4 WS-X6066-SLB-APC SAD105003DW Hw : 1.9
Fw :
Sw : 4.2(2)

Module	DRAM			FLASH			NVRAM		
	Total	Used	Free	Total	Used	Free	Total	Used	Free
1	262144K	70354K	191790K	32768K	23251K	9517K	512K	253K	259K

Uptime is 43 days, 22 hours, 7 minutes

The following configuration segment shows a vserver with service terminations enabled:

```
vserver WWW:2  
  virtual x.x.x.x tcp www service termination
```

☐ Products Confirmed Not Vulnerable

Only Catalyst CSM modules running indicated 4.2 versions are affected by these vulnerabilities. CSM software versions 4.1, 3.2 and 3.1 are not affected by these vulnerabilities.

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

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 Catalyst CSM is an integrated Server Load Balancing line card for the Catalyst 6500 and 7600 Series 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 Catalyst 6500 CSM-S combines high-performance server load balancing (SLB) with Secure Socket Layer (SSL) offload. The CSM-S is similar to the CSM; however, it can also terminate and initiate SSL-encrypted traffic, which allows the CSM-S to perform intelligent load balancing while ensuring secure end-to-end encryption.

When a module running affected code receives specific TCP packets out of order, a DoS condition may be triggered resulting in the CPU reaching 100% utilization or a reload with a FPGA4 exception with icp.fatPath length error.

This vulnerability is documented in Cisco bug ID [CSCsd27478](#) ([registered customers only](#)) .

When service termination is enabled on a module running affected software and the module is under high network utilization, a DoS condition may be triggered, resulting in a reload with a FPGA4

exception 1 IDLE error.

This vulnerability is documented in Cisco bug ID [CSCsh57876](#) (**registered customers only**) .

In normal operations, the MSFC CLI handles the management of the CSM and CSM-S; however, in order to upgrade the software, a user must first log into the switch and session to the module.

For more information on how to upgrade your CSM, visit the http://www.cisco.com/en/US/products/hw/modules/ps2706/products_tech_note09186a0080094526.s page on Cisco.com.

Information on how to upgrade the CSM-S can be found at: http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/csms/2.1.1/configuration/gu

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

☐ Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities 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.

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

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

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>.

FPGA4 exception under high network utilization and service termination is enabled					
Calculate the environmental score of CSCsh57876					
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

FPGA4 exception with icp.fatPath length error when out of order packets are received					
Calculate the environmental score of CSCsd27478					
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 these vulnerabilities against a system running a vulnerable version of CSM or CSM-S software may cause the system to become unresponsive or reload. Repeated attacks may result in a prolonged DoS condition.

[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.

For more information on the terms "Rebuild" and "Maintenance," consult the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e

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

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

☐ **Workarounds**

There are no workarounds for these vulnerabilities. Removing service termination will mitigate Cisco bug ID [CSCsh57876](#); however, disabling this feature disables services that may be critical to the operation of the device.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20070905-csm.shtml>

☐ **Obtaining Fixed Software**

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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

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.

[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.

These vulnerabilities were 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-20070905-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 1.1	2008-April-25	Updated links to the CVSS scores for CSCsh57876 and CSCsd27478 .
Revision 1.0	2007-Sept-05	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
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)