

Cisco Security Advisory: Firewall Services Module Crafted ICMP Message Vulnerability

Advisory ID: cisco-sa-20090819-fwsm

<http://www.cisco.com/warp/public/707/cisco-sa-20090819-fwsm.shtml>

Revision 1.0

For Public Release 2009 August 19 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

A vulnerability exists in the Cisco Firewall Services Module (FWSM) for the Catalyst 6500 Series Switches and Cisco 7600 Series Routers. The vulnerability may cause the FWSM to stop forwarding traffic and may be triggered while processing multiple, crafted ICMP messages.

There are no known instances of intentional exploitation of this vulnerability. However, Cisco has observed data streams that appear to trigger this vulnerability unintentionally.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090819-fwsm.shtml>.

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

☐ Affected Products

☐ Vulnerable Products

All non-fixed 2.x, 3.x and 4.x versions of the FWSM software are affected by this vulnerability.

To determine the version of the FWSM software that is running, issue the **show module** command-line interface (CLI) command from Cisco IOS Software or Cisco Catalyst Operating System Software to identify what modules and sub-modules are installed in the system.

The following example shows a system with an FWSM (WS-SVC-FWM-1) installed in slot 4.

```
switch#show module
  Mod Ports Card Type
Model                Serial No.
-----
1      48    SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-
TX      Sxxxxxxxxx
4       6     Firewall Module                               WS-SVC-FWM-
1      Sxxxxxxxxx
5       2     Supervisor Engine 720 (Active)              WS-SUP720-
BASE    Sxxxxxxxxx
6       2     Supervisor Engine 720 (Hot)                  WS-SUP720-
BASE    Sxxxxxxxxx
```

After locating the correct slot, issue the **show module <slot number>** command to identify the software version that is running.

```
switch#show module 4
  Mod Ports Card Type
Model                Serial No.
-----
4       6     Firewall Module                               WS-SVC-FWM-
1      Sxxxxxxxxx

  Mod MAC addresses          Hw      Fw
Sw      Status
-----
4      0003.e4xx.xxxx to 0003.e4xx.xxxx  3.0    7.2(1)    3.2
(3)    Ok
```

The preceding example shows that the FWSM is running software version 3.2(3) as indicated by the column under "Sw".

Note: Recent versions of Cisco IOS Software will show the software version of each module in the output from the **show module** command; therefore, executing the **show module <slot number>** command is not necessary.

If a Virtual Switching System (VSS) is used to allow two physical Cisco Catalyst 6500 Series Switches to operate as a single logical virtual switch, the **show module switch all** command can display the software version of all FWSMs that belong to switch 1 and switch 2. The output from this command will be similar to the output from the **show module <slot number>** but will include module information for the modules in each switch in the VSS.

Alternatively, version information can be obtained directly from the FWSM through the **show version** command, as shown in the following example.

```
FWSM#show version
FWSM Firewall Version 3.2(3)
```

Customers who use the Cisco Adaptive Security Device Manager (ASDM) to manage their devices can find the version of the software displayed in the table in the login window or in the upper left corner of the ASDM window. The version notation is similar to the following example.

```
FWSM Version: 3.2(3)
```

☐ Products Confirmed Not Vulnerable

Other Cisco products that offer firewall services, including Cisco IOS Software, Cisco ASA 5500 Series Adaptive Security Appliances, and Cisco PIX Security Appliances, are **not** affected by this vulnerability.

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

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

☐ Details

The Cisco FWSM is a high-speed, integrated firewall module for Catalyst 6500 Series Switches and Cisco 7600 Series Routers. The FWSM offers firewall services with stateful packet filtering and deep packet inspection.

A vulnerability exists in the Cisco FWSM Software that may cause the FWSM to stop forwarding traffic between interfaces, or stop processing traffic that is directed at the FWSM (management traffic) after multiple, crafted ICMP messages are processed by the FWSM. Any traffic that transits or is directed towards the FWSM is affected, regardless of whether ICMP inspection (**inspect icmp** command under Class configuration mode) is enabled.

The FWSM stops processing traffic because one of the Network Processors (NPs) that is used by the FWSM to handle traffic may use all available execution threads while handling a specific type of crafted ICMP messages. This behavior limits the execution threads that are available to handle additional traffic.

Administrators may be able to determine if the FWSM has been affected by this vulnerability by issuing the **show np 2 stats** command. If this command produces output showing various counters and their values, as shown in the example CLI output that follows, the FWSM has not been affected by the vulnerability. If the command returns a single line that reads "ERROR: np_logger_query request for FP Stats failed", the FWSM may have been affected by the vulnerability.

```
FWSM#show np 2 stats
```

```
-----  
PKT_MNG: total packets (dot1q) rcvd           : 10565937  
PKT_MNG: total packets (dot1q) sent           : 4969517  
PKT_MNG: total packets (dot1q) dropped        : 65502  
PKT_MNG: TCP packets received                 : 0  
PKT_MNG: UDP packets received                 : 4963509  
PKT_MNG: ICMP packets received                : 0  
PKT_MNG: ARP packets received                 : 2  
PKT_MNG: other protocol pkts received         : 0  
PKT_MNG: default (no IP/ARP) dropped           : 0  
SESS_MNG: sessions created                     : 18  
SESS_MNG: sessions embryonic to active        : 0  
...  

```

An FWSM that stops processing traffic as a result of this vulnerability will need to be reloaded. Administrators can reload the FWSM from the supervisor of the Catalyst 6500 Series Switch or the Cisco 7600 Series Router by issuing the command **hw-module module <slot # for FWSM> reset** (Cisco IOS Software), or **set module power up/down <module #>** (Cisco CatOS Software). Note that unless the FWSM software is updated to a non-vulnerable version, or crafted ICMP messages are blocked (see the Workarounds section for details), the FWSM can still be subject to exploitation (intentional or otherwise) after a reload.

If an FWSM that is configured for failover operation encounters this issue, the active FWSM may not properly fail over to the standby FWSM.

IPv6 (in particular ICMPv6) cannot trigger this vulnerability.

This issue is documented in Cisco Bug ID [CSCsz97207](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2009-0638.

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

☐ 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 a 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>

CSCsz97207 -- NP 2 threads lock due to processing malformed IP packet

Calculate the environmental score of [CSCsz97207](#)

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 the vulnerability may cause the FWSM to stop forwarding traffic between interfaces (transit traffic), and stop processing traffic directed at the FWSM (management traffic). If the FWSM is configured for failover operation, the active FWSM may not fail over to the standby FWSM.

[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.

Each row of the FWSM software table below describes a major FWSM software train and the earliest possible release within that train that contains the fix (the "First Fixed Release") and the anticipated date of availability (if not currently available) in the "First Fixed Release" column. A device running a release that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

Major Release	First Fixed Release
2.x	Vulnerable; migrate to 3.x or 4.x
3.1	3.1(16)
3.2	3.2(13)
4.0	4.0(6)

Fixed FWSM software can be downloaded from the Software Center on cisco.com by visiting <http://www.cisco.com/kobayashi/sw-center/index.shtml> and navigating to "Security" > "Cisco Catalyst 6500 Series Firewall Services Module" > "Firewall Services Module (FWSM) Software".

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

Workarounds

There are no workarounds for this vulnerability. Access control lists (ACLs) that are deployed on the FWSM itself to block through-the-device or to-the-device ICMP messages are not effective to prevent this vulnerability. However, blocking unnecessary ICMP messages on screening devices or on devices in the path to the FWSM will prevent the FWSM from triggering the vulnerability. For example, the following ACL, when deployed on a Cisco IOS device in front of the FWSM, will prevent crafted ICMP messages from reaching the FWSM, and thus protect the FWSM from triggering the vulnerability:

```
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any traceroute
access-list 101 permit icmp any any packet-too-big
access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any host-unreachable
access-list 101 permit icmp any any unreachable
access-list 101 deny icmp any any
access-list 101 permit ip any any
```

This sample ACL is allowing certain ICMP messages that are vital for network troubleshooting and for proper operation of the network. It is safe to allow any other ICMP messages for which the Cisco IOS Software **access-list** command has named ICMP type keywords. ACLs like the one in the preceding example may also be deployed on non-Cisco IOS devices, such as the Cisco PIX and ASA security appliances, although the ACL syntax on non-Cisco IOS devices may not support all the named ICMP type keywords that the Cisco IOS ACL syntax supports. However, on non-Cisco IOS devices, it is safe to permit all ICMP messages for which there are named ICMP type keywords in the ACL syntax.

As mentioned in the Details section, if the FWSM has stopped processing traffic due to this vulnerability, the FWSM will require a reload. Administrators can reload the FWSM by logging in to the supervisor of the Catalyst 6500 Series Switch or the Cisco 7600 Series router and issuing the **hw-module module <slot # for FWSM> reset** (Cisco IOS Software), or **set module power up/down <module #>** (Cisco CatOS Software) commands.

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, which is available at the following link: <http://www.cisco.com/warp/public/707/cisco-amb-20090819-fwsm.shtml>.

[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/en/US/support/tsd_cisco_worldwide_contacts.html 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, but Cisco is aware of customers that have encountered this vulnerability during normal network operation.

This vulnerability was discovered during the handling 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-20090819-fwsm.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-bulletins@lists.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	2009-August-19	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

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)