

# Cisco Security Advisory: Application Inspection Vulnerability in Cisco Firewall Services Module

Advisory ID: cisco-sa-20071219-fwsm

<http://www.cisco.com/warp/public/707/cisco-sa-20071219-fwsm.shtml>

## Revision 1.2

Last Updated 2008 January 3 1600 UTC (GMT)

For Public Release 2007 December 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: Interim](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Summary

A vulnerability exists in the Cisco Firewall Services Module (FWSM) - a high-speed, integrated firewall module for Cisco Catalyst 6500 switches and Cisco 7600 Series routers, that may result in a reload of the FWSM. The only affected FWSM System Software Version is 3.2(3).

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

Common Vulnerabilities and Exposures (CVE) identifier CVE-2007-5584 has been assigned to this vulnerability.

Cisco will release free software updates that address this vulnerability.

A workaround that mitigates this vulnerability is available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20071219-fwsm.shtml>.

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

## ☐ Affected Products

### ☐ Vulnerable Products

The FWSM is vulnerable if running System Software version 3.2(3).

To determine if the FWSM is vulnerable, issue the **show module** command-line interface (CLI) command from Cisco IOS or Cisco CatOS to identify what modules and sub-modules are installed in the system.

The following example shows a system with a Firewall Service Module (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   Sxxxxxxxxxxx
 4    6   Firewall Module                               WS-
SVC-FWM-1     Sxxxxxxxxxxx
 5    2   Supervisor Engine 720 (Active)              WS-
SUP720-BASE   Sxxxxxxxxxxx
 6    2   Supervisor Engine 720 (Hot)                 WS-
SUP720-BASE   Sxxxxxxxxxxx

```

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           Sxxxxxxxxxxx

  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 version 3.2(3) as indicated by the column under "Sw" above.

Note: Recent versions of Cisco IOS 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.

Alternatively, the information can also be obtained directly from the FWSM through the show version command as seen 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

- FWSM System Software versions 3.2(2) and earlier.
- FWSM System Software versions 3.1(x).
- FWSM System Software versions 1.x(y) and 2.x(y).
- Cisco PIX 500 Series Security Appliance (PIX).
- Cisco 5500 Series Adaptive Security Appliance (ASA).

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

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

## ☐ Details

A vulnerability exists in the processing of data in the control-plane path with Layer 7 Application Inspections, that may result in a reload of the FWSM. The vulnerability can be triggered with standard network traffic, which is passed through the Application Layer Protocol Inspection process.

The only FWSM release affected by this vulnerability is FWSM System Software version 3.2(3).

This vulnerability is documented in Cisco bug ID [CSCsl08519](#) ( [registered](#) customers only) .

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

## ☐ Vulnerability Scoring Details

Cisco has provided 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.

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>.

<b>CSCs108519 - FWSM Version 3.2.3 System Software may crash with Application Layer Protocol Inspection</b>					
<b>Calculate the environmental score of <a href="#">CSCs108519</a></b>					
<b>CVSS Base Score - 7.8</b>					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
<b>CVSS Temporal Score - 7</b>					
Exploitability		Remediation Level		Report Confidence	
Functional		Workaround		Confirmed	

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

## [-] Impact

Successful exploitation of the vulnerability may result in a reload of the FWSM. Repeated exploitation will result in a sustained denial of service attack.

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

## [-] Software Versions and Fixes

When considering software upgrades, 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.

FWSM software version 3.2(4) contains the fixes for the vulnerability described in this document and will be available for download during the week beginning 7th January 2008.

FWSM software will be available for download from the following location on cisco.com: <http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm?psrtdcat20e2> ( [registered](#) customers only) .

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

## ☐ Workarounds

### Disable the TCP Normalizing Function

Disabling the TCP normalizing function in the FWSM will mitigate this vulnerability.

The TCP normalizer performs the following action:

For traffic that passes through the control-plane path, such as packets that require Layer 7 inspection or management traffic, the FWSM sets the maximum number of out-of-order packets that can be queued for a TCP connection to two packets. The TCP normalizer is enabled by default and is not configurable except to enable or disable.

To disable the TCP normalizing function, use the **no control-point tcp-normalizer** command in global configuration mode, as shown in the following example.

```
FWSM# config terminal
FWSM(config)# no control-point tcp-normalizer
FWSM(config)#
FWSM#
```

Disabling the "control-point tcp-normalizer" will prevent strict TCP checks, such as detecting out-of-sequence segments and monitoring TCP options, on the TCP packets received on the Control Plane for Layer 7 inspection in the FWSM, will not be performed. The feature should be re-enabled after upgrading to a fixed version of software.

## ☐ **Obtaining Fixed Software**

Cisco will release free software updates that address these vulnerabilities. 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](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](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto: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](mailto: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**

This issue was first discovered via internal testing at Cisco. There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability.

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

## ☐ **Status of this Notice: Interim**

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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-20071219-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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 1.2	2008-January-3	Updated the download availability date of the Software Versions and Fixes section.
Revision 1.1	2007-December-19	Updated the temporal score section of the CVSS table.
Revision 1.0	2007-December-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](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](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)