

[Solutions](#)[Products](#)[Ordering](#)[Support](#)[Partners](#)[Training](#)[Corporate](#)[Security Advisories](#)

Cisco Security Advisory: Multiple Vulnerabilities in Firewall Services Module

Advisory ID: cisco-sa-20070214-fwsm

<http://www.cisco.com/warp/public/707/cisco-sa-20070214-fwsm.shtml>

Revision 1.4

Last Updated 2007 June 20 1336 UTC (GMT)

For Public Release 2007 February 14 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Version and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Multiple vulnerabilities exist in the Cisco Firewall Services Module (FWSM). These vulnerabilities occur in the processing of specific Hypertext Transfer Protocol (HTTP), Secure HTTP (HTTPS), Session Initiation Protocol (SIP), and Simple Network Management Protocol (SNMP) traffic. If verbose logging is enabled for debugging purposes, a vulnerability exists when the FWSM processes packets destined to itself. All of these vulnerabilities may result in a reload of the device.

An additional vulnerability is included in this advisory in which the manipulation of access control lists (ACLs) that make use of object groups may corrupt the ACL and create a situation where unwanted traffic may be permitted or desirable traffic may be blocked.

These vulnerabilities are independent of each other; a release that is affected by one vulnerability is not necessarily affected by the others.

There are workarounds for some of the vulnerabilities disclosed in this advisory.

Cisco has made free software available to address this issue for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070214-fwsm.shtml>

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

☐ Affected Products

The vulnerabilities described in this document apply to the FWSM. The companion advisory <http://www.cisco.com/warp/public/707/cisco-sa-20070214-pix.shtml> contains information about similar vulnerabilities that affect the Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances.

☐ Vulnerable Products

The following table indicates which software releases for the Cisco FWSM are affected and under what conditions:

Vulnerability Name	Only affected if...	Vulnerable by default?	Versions affected	Cisco Bug ID
1. Enhanced Inspection of Malformed HTTP Traffic May Cause Reload	Enhanced inspection of HTTP traffic is enabled through the command inspect http <i><appfw></i>	No	All 3.x software releases prior to 3.1(3.24)	CSCsd75794
2. Inspection of Malformed SIP Messages	SIP inspection is enabled through the command fixup protocol sip <i><portnum></i> and/or fixup protocol sip udp <i><portnum></i> (in	Yes	All software releases prior to 2.3(4.12)	CSCsg80915

May Cause Reload	FWSM software 2.x and before) or through the command inspect sip (in FWSM software 3.x and later)		and all 3.x releases prior to 3.1(3.24)	
3. Processing of Packets Destined to the FWSM May Cause Reload	Logging at "debugging" level (regardless of the logging destination) and syslog message 710006 is enabled	No	All 3.x software releases prior to 3.1(3.3)	CSCse85707
4. Processing of Malformed HTTPS Traffic May Cause Reload	Network access authentication is enabled through the aaa authentication match or aaa authentication include commands	No	All 3.x software releases prior to 3.1(3.18)	CSCsg50228
5. Processing of Long HTTP Requests May Cause Reload	Network access authentication is enabled through the aaa authentication match or aaa authentication include commands	No	All 3.x releases prior to 3.1(2)	CSCsd91268
6. Processing HTTPS Traffic May Cause a Reload	HTTPS server is enabled through the http server enable command	No	All 3.x releases prior to 3.1(3.11)	CSCsf29974
	SNMP traffic			

7. Processing of Malformed SNMP Requests May Cause a Reload	from a particular IP address is permitted through the command snmp-server host <interface name> <IP address of SNMP server>	No	All 3.x releases prior to 3.1(3.1)	CSCse52679
8. Manipulation of ACL May Cause ACL Corruption	ACL makes use of object groups and ACL is manipulated by an administrator	No	All software releases prior to 2.3(4.7) and all 3.x releases prior to 3.1(3.1)	CSCse60868 , CSCse99740 and CSCsd50667

The relationship between the vulnerabilities described in this advisory and the equivalent vulnerabilities in the Cisco PIX 500 Series Security Appliances and Cisco ASA 5500 Series Adaptive Security Appliances is given in the following table. If a vulnerability discussed in this document is not present in this table, it *does not affect* the Cisco PIX 500 Series Security Appliances and Cisco ASA 5500 Series Adaptive Security Appliances.

Vulnerability	PIX/ASA Bug ID	FWSM Bug ID
Enhanced Inspection of Malformed HTTP Traffic May Cause Reload	CSCsd75794	CSCsd75794
Inspection of Malformed SIP Messages May Cause Reload	CSCse27708 and CSCsd97077	CSCsg80915

To determine if you are running a vulnerable version of FWSM software, issue the **show module** command in IOS or CatOS to identify what modules and sub-modules are installed in the system.

The example below shows a system with a Firewall Service Module (WS-SVC-FWM-1) installed in slot 4.

```
6506-B#show module
Mod Ports Card Type                               Model                               Serial
```

```

-----
1  48  SFM-capable 48 port 10/100/1000mb RJ45  WS-X6548-GE-TX      SAxxxx
4   6   Firewall Module                               WS-SVC-FWM-1       SAxxxx
5   2   Supervisor Engine 720 (Active)           WS-SUP720-BASE    SAxxxx
6   2   Supervisor Engine 720 (Hot)              WS-SUP720-BASE    SAxxxx
-----

```

After locating the correct slot, issue the **show module <slot number>** command to identify the version of software running:

```

6506-B#sho module 4
Mod Ports Card Type                               Model                               Serial
-----
4   6   Firewall Module                               WS-SVC-FWM-1                       SAxxxx

Mod MAC addresses                               Hw   Fw           Sw           S
-----
4   0003.e4xx.xxxx to 0003.e4xx.xxxx          3.0  7.2(1)      2.3(1)      Ok

```

In this example, the FWSM is running version 2.3(1) as indicated by the column under "Sw" above.

Note: recent versions of IOS will show the software version of each module in the output from the **show module** command so executing the **show module <slot number>** command is not necessary.

Alternatively, the information may also be gained directly from the FWSM through the **show version** command:

```

FWSM#show version

FWSM Firewall Version 2.3(1)

```

For customers managing their FWSM through the PIX Device Manager (PDM) or the Cisco Adaptive Security Device Manager (ASDM), log into the application, and the version may be found either in the table in the login window or in the upper left hand corner of the PDM/ASDM window indicated by a label similar to:

```
FWSM Version: 2.3(1)
```

☐ Products Confirmed Not Vulnerable

With the exception of the Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances, no other Cisco products are known to be vulnerable to the issues described in this advisory.

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

☐ Details

The Cisco Firewall Services Module is a high-speed, integrated firewall module for Catalyst 6500 series switches and Cisco 7600 series routers. It offers firewall services with stateful packet filtering and deep packet inspection.

Multiple vulnerabilities exist in certain versions of the FWSM software that may cause the device to unexpectedly reload or that may cause traffic to be permitted or denied contrary to the security policy in place.

1. Enhanced Inspection of Malformed HTTP Traffic May Cause Reload

This vulnerability may cause a FWSM to reload when the FWSM performs *enhanced* inspection of HTTP requests, and a malformed HTTP request is inspected by the FWSM. The FWSM only performs enhanced inspection of HTTP traffic when the command **inspect http <appfw>** is present in the configuration (*appfw* is the name of a specific HTTP map.) This command is disabled by default.

Note: Enhanced inspection of HTTP traffic is what makes a configuration affected. Regular inspection of HTTP traffic (through the command **inspect http** without an HTTP map) will not make a configuration affected by this vulnerability.

For information on what enhanced inspection of HTTP traffic does, and how to configure it, please refer to the following URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_ch

This vulnerability is documented in Cisco Bug ID [CSCsd75794](#) ([registered](#) customers only) .

2. Inspection of Malformed SIP Messages May Cause Reload

This vulnerability may cause a FWSM to reload when a malformed SIP message is received (over Transmission Control Protocol [TCP] or over User Datagram Protocol [UDP]) and deep packet inspection of SIP messages is enabled through the commands **fixup protocol sip <portnum>** for SIP over TCP and/or **fixup protocol sip udp <portnum>** for SIP over UDP (in FWSM software 2.3.x and before) or through the command **inspect sip** (in FWSM software 3.x and later). SIP fixup (in 2.x and earlier) and SIP inspection (in 3.x and later) are enabled by default.

This vulnerability is documented in Cisco Bug ID [CSCsg80915](#) ([registered](#) customers only) .

3. Processing of Packets Destined to the FWSM May Cause Reload

This vulnerability will cause the FWSM to reload when trying to generate syslog message 710006. For this to happen the following two conditions must be satisfied:

- The FWSM receives a packet for one of the device's IP addresses and the message is not one of the following protocols: TCP, UDP, ICMP, OSPF, Failover, PIM, IGMP, and ESP. The source of the packet is not relevant.
- Logging must be enabled at a level high enough to generate syslog message 710006. By default this is debugging level (level 7). Please note that logging is disabled by default, and Cisco recommends customers only log at debugging level for debugging and troubleshooting purposes.

Note: The documentation for the Cisco Security Monitoring, Analysis and Response System (CS-MARS) suggests logging at the debugging level so more events can be reported by the firewall.

For more information on syslog message 710006 please refer to the following document:

- Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages, 3.1
http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guide_cl

This vulnerability is documented in Cisco Bug ID [CSCse85707](#) ([registered](#) customers only) .

4. Processing of Malformed HTTPS Requests May Cause Reload

This vulnerability may cause the FWSM to reload when a user tries to access a web site and the network administrator has configured the device to authenticate users before granting them network access. This feature is known as "authentication for network access", or *auth-proxy*, and is enabled through the command **aaa authentication match** or **aaa authentication include**.

The reload is actually triggered by a specific HTTPS request that is invalid, and therefore, unlikely to be generated by a regular web browser.

This vulnerability is documented in Cisco Bug ID [CSCsg50228](#) ([registered](#) customers only) .

5. Processing of Long HTTP Requests May Cause Reload

This vulnerability may also cause the FWSM to reload when the administrator has enabled "authentication for network access ("auth-proxy") through the commands **aaa authentication match** or **aaa authentication include**. However, in this case, the HTTP request that causes the reload is valid, although it is not a normal request in the sense that the URL being requested is very long. A web browser could potentially generate such a request during regular browsing.

This vulnerability is documented in Cisco Bug ID [CSCsd91268](#) ([registered](#) customers only) .

6. Processing of HTTPS Traffic May Cause Reload

This vulnerability may cause a FWSM to reload when the FWSM receives a particular type of HTTPS traffic directed to the FWSM itself. This is only a concern when the HTTPS server on the FWSM is enabled through the command **http server enable**. This command is disabled by default.

Cisco is aware of a commercial vulnerability scanner that can generate the HTTPS traffic that triggers the reload. We are not aware of regular web browser traffic that triggers this bug.

This vulnerability is documented in Cisco Bug ID [CSCsf29974](#) ([registered](#) customers only) .

7. Processing of Malformed SNMP Requests May Cause a Reload

This vulnerability may cause a FWSM to reload upon receipt of a malformed SNMP message from a trusted device. The trusted device must be allowed explicit SNMP poll access via the command **snmp-server host <interface name> <IP of trusted device>**.

This vulnerability is documented in Cisco Bug IDs [CSCse52679](#) ([registered](#) customers only) .

8. Manipulation of ACL May Cause ACL Corruption

This vulnerability may cause access control entries (ACEs) in an ACL to be evaluated out of order, or not to be evaluated. This ACL corruption is manifested, besides the obvious traffic implications, when the output from the **show access-list** command and the corresponding ACL shown by the **show running-config** command appear to be out of sync. Only a manual reload of the device will cause this condition to go away.

The ACL corruption occurs when an ACL that makes use of object groups is manipulated.

This vulnerability is documented in Cisco Bug IDs [CSCse60868](#) ([registered](#) customers only) , [CSCse99740](#) ([registered](#) customers only) and [CSCsd50667](#) ([registered](#) customers only) .

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS).

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.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.


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>.


CSCsd75794 - Enhanced inspection of Malformed HTTP traffic can crash device						
Calculate the environmental score of CSCsd75794 ↗						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

[CSCsg80915 - FWSM - Traceback when inspecting SIP packets](#)


Calculate the environmental score of CSCsg80915 						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		


CSCse85707 - FWSM crash when printing debug level syslog 710006						
Calculate the environmental score of CSCse85707 						
CVSS Base Score - 2.7						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	High	Not Required	None	None	Complete	Normal
Temporal Score - 2.2						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		


CSCsg50228 - FWSM ST MODE crashes at Thread NAME: uauth with RADIUS						
Calculate the environmental score of CSCsg50228 						
CVSS Base Score - 2.7						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	High	Not Required	None	None	Complete	Normal
Temporal Score - 2.2						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

CSCsd91268 - FWSM crashes at Thread: uauth while using aaa with TACACS						
Calculate the environmental score of CSCsd91268 						
CVSS Base Score - 10						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias

Remote	Low	Not Required	Complete	Complete	Complete	Normal
Temporal Score - 8.3						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

CSCsf29974 - Crash in emweb/https thread						
Calculate the environmental score of CSCsf29974 						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

CSCse52679 - FWSM Crash in thread name SNMP						
Calculate the environmental score of CSCse52679 						
CVSS Base Score - 3.3						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	None	None	Complete	Normal
Temporal Score - 2.7						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

CSCse60868 - Modifying an ACL with an object-group could cause ACL corruption , CSCse99740 - When removing network objects the existing ACL lines are not removed and CSCsd50667 - ACLs block traffic although explicit allowed						
Calculate the environmental score of CSCse60868 , CSCse99740 and CSCsd50667 						
CVSS Base Score - 3.2						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	High	Required	Complete	Complete	None	Normal
Temporal Score - 2.6						

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

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

☐ Impact

In all cases, with the exception of the "Manipulation of ACL May Cause ACL Corruption" vulnerability, successful exploitation of any vulnerability may cause a reload of the affected device. Repeated exploitation could result in a sustained Denial-of-Service (DoS) condition.

In the case of the "Processing of Long HTTP Requests May Cause Reload" vulnerability ([CSCsd91268](#)), the reload occurs because a stack-based buffer is overflowed. In this case remote code execution may be possible.

In the case of the "Manipulation of ACL May Cause ACL Corruption" vulnerability, a device that becomes affected after an administrator manipulates an ACL with object groups may allow traffic that would normally be denied, or would deny traffic that would normally be permitted. If the ACL is used for other functions like NAT (policy NAT and NAT exemption), AAA (auth-proxy), control of access to the device (SSH, Telnet, HTTP, ICMP), then those functions may be adversely affected as well.

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

☐ Software Version 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 one of the vulnerabilities described in this document. For each vulnerability the earliest possible release that contains the fix (the "First Fixed Release") and the anticipated date of availability for each are listed 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).

Vulnerability	First Fixed Release
1. Enhanced Inspection of Malformed HTTP Traffic May Cause Reload (CSCsd75794)	3.1(3.24) (the 2.3.x series are not affected)
2. Inspection of Malformed SIP	2.3(4.12) for the

Messages May Cause Reload (CSCsg80915)	2.3.x series, and 3.1(3.24) for the 3.x series
3. Processing of Packets Destined to the FWSM May Cause Reload (CSCse85707)	3.1(3.3) (the 2.3.x series are not affected)
4. Processing of Malformed HTTPS Requests May Cause Reload (CSCsg50228)	3.1(3.18) (the 2.3.x series are not affected)
5. Processing of Long HTTP Requests May Cause Reload (CSCsd91268)	3.1(1.9) (the 2.3.x series are not affected)
6. Processing HTTPS Traffic May Cause a Reload (CSCsf29974)	3.1(3.11) (the 2.3.x series are not affected)
7. Processing of Malformed SNMP Requests May Cause a Reload (CSCse52679)	3.1(3.1) (the 2.3.x series are not affected)
8. Manipulation of ACL May Cause ACL Corruption (CSCse60868) , (CSCse99740) and (CSCsd50667)	2.3(4.7) for the 2.3.x series, and 3.1(3.1) for the 3.x series

For the 2.3.x series, FWSM software version 2.3(4.12) contains the fixes for all the vulnerabilities described in this document.

For the 3.x series, FWSM software version 3.1(4) contains the fixes for all the vulnerabilities described in this document.

FWSM software is available for download from the following location on cisco.com:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fws?psrtdcat20e2>

For FWSM release 2.3(4.12) please use the following link:

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

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

☐ Workarounds

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-20070214-firewall.shtml>

1. Enhanced Inspection of Malformed HTTP Traffic May Cause Reload

It is possible to mitigate this vulnerability by disabling enhanced inspection of HTTP traffic. Please note that disabling HTTP enhanced inspection will prevent the FWSM from protecting against specific attacks and other threats that may be associated with HTTP traffic. Enhanced inspection of HTTP traffic is disabled by removing the command **inspect http <appfw>** from the configuration, where *appfw* is the name of an HTTP map.

For further information about the **inspect http <appfw>** command, and the type of checks it performs on HTTP traffic, please see the documentation for this command at:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter091

Please note that the command **inspect http** (without an HTTP map) can be left in the configuration and the device will not be affected by this vulnerability.

2. Inspection of Malformed SIP Messages May Cause Reload

It is possible to mitigate this vulnerability by disabling deep packet inspection ("fixup" in software version prior to 3.x or "inspect" in software version 3.x and later) of SIP messages. In FWSM software 2.x and earlier, it is necessary to use both **no fixup protocol sip** and **no fixup protocol sip udp** to stop deep packet inspection of SIP messages over TCP and UDP transport (in FWSM 3.x and later **no inspect sip** will stop deep packet inspection of SIP messages over both TCP and UDP.) Note, however, that this may have negative impact on devices terminating SIP sessions since SIP traffic will no longer undergo stateful application inspection, and devices which terminate sessions for this protocol will be exposed to packets that may cause these devices to crash or become compromised.

If you are running a 3.x FWSM software release, then the alternative is to allow traffic only from the trusted hosts. The configuration to accomplish this is as follows:

```
access-list sip-acl extended permit udp 10.1.1.0 255.255.255.0 host 192.168.
access-list sip-acl extended permit udp host 192.168.5.4 10.1.1.0 255.255.25

class-map sip-traffic
  match access-list sip-acl
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect esmtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect netbios
    inspect tftp
  class sip-traffic
    inspect sip
!
```

```
service-policy global_policy global
```

In this example SIP endpoints are any host within 10.1.1.0 network (inside the trusted network) and a host with the IP address of 192.168.5.4 (outside of the trusted network). You would have to substitute these IP addresses with the ones that are used in your network.

Please note that SIP is an UDP-based protocol, so spoofing SIP messages is possible.

3. Processing of Packets Destined to the FWSM May Cause Reload

Since this vulnerability only manifests itself when syslog message 710006 is generated, it is possible to workaround the vulnerability either by disabling generation of syslog message 710006 altogether, or by logging at a syslog level that is lower than the syslog level at which this message is generated.

By default, syslog message 710006 is generated at syslog level 7 ("debugging"), so a viable workaround is to log at level 6 or lower. This can be accomplished with the command **logging <destination> 6**. If syslog message 710006 has been moved to a different logging level, then the logging level in use must be changed accordingly to prevent the message from being generated.

If logging at the "debugging" level is necessary, the vulnerability can also be eliminated by disabling this particular syslog message by using the command **no logging message 710006**.

4. Processing of Malformed HTTPS Requests May Cause Reload

There are no workarounds for this vulnerability.

5. Processing of Long HTTP Requests May Cause Reload

There are no workarounds for this vulnerability.

6. Processing HTTPS Traffic May Cause a Reload

Since this vulnerability is caused by the HTTPS server on the FWSM failing to handle certain types of HTTPS traffic, disabling the HTTPS server through the command **no http server enable** is a valid workaround if this functionality is not needed. Please note that this functionality is used by ASDM, so if configuration of the FWSM is exclusively done through ASDM disabling the HTTPS server may not be a viable workaround.

Additionally, it is possible to limit the exposure by allowing HTTPS connections only from trusted IP addresses or networks. This can be accomplished with the **http** command. For example, the following command:

```
FWSM(config)# http 192.168.1.10 255.255.255.255 inside
```

will only permit HTTPS connections from the IP address 192.168.1.10.

7. Processing of Malformed SNMP Requests May Cause a Reload

This bug can only be triggered by a malformed SNMP message that comes from a device that is allowed SNMP access on the FWSM. If SNMP is not needed it can be removed through the command **no snmp-server host <interface name> <IP address of trusted device>**, which will eliminate the vulnerability.

8. Manipulation of ACL May Cause ACL Corruption

There are no workarounds for this vulnerability. However, please note that the ACL corruption does not occur during normal operation of the device and it cannot be triggered by some type of traffic. It can only occur if an administrator makes configuration changes (and more specifically, if an administrator manipulates an ACL.) For this reason, if ACL changes are made only during a maintenance window, and the FWSM is reloaded after making those changes, there should not be any concerns with this vulnerability.

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

☐ 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.

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

☐ 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>.

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

☐ 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.

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

☐ **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.

Some of these vulnerabilities were reported to Cisco by customers that experienced these issues during normal operation of their equipment. The other vulnerabilities were discovered during internal testing.

[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-20070214-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-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 1.4	2007-Jun-20	Added information about CSCsd50667 - duplicate of CSCse99740 - to be consistent with the FWSM release notes.
Revision 1.3	2007-Feb-23	Clarify that the "Inspection of Malformed SIP Messages May Cause Reload" vulnerability affects SIP traffic over both TCP and UDP transport, and that a configuration may be affected for both, depending on the commands used. The workaround of disabling SIP may also require removing two commands.
		It was incorrectly stated in previous versions of this document that SIP inspection is disabled by default in FWSM 3.x software. The advisory has

Revision 1.2	2007-Feb-21	been revised to make it clear that the "Inspection of Malformed SIP Messages May Cause Reload" vulnerability affects the default configuration in both 2.x and 3.x software.
Revision 1.1	2007-Feb-14	Revised CVSS scores for CSCsd91268 (to reflect Remote Code Execution potential) and for CSCse60868 and CSCse99740 (to reflect that authentication is required).
Revision 1.0	2007-Feb-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](#)

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.](#)