

Cisco Security Advisory: FWSM URL Filtering Solution TCP ACL Bypass Vulnerability

Document ID: 64821

Advisory ID: cisco-sa-20050511-url

<http://www.cisco.com/warp/public/707/cisco-sa-20050511-url.shtml>

Revision 1.0

For Public Release 2005 May 11 1600 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[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 Firewall Services Module (FWSM) is a high-speed, integrated firewall module for Catalyst 6500 series switches and Cisco 7600 series routers. A vulnerability exists in the Cisco Firewall Services Module when URL, FTP, or HTTPS filtering is enabled in which inbound TCP packets can bypass access-list entries intended to explicitly filter them.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050511-url.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

Only Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Internet Routers with a Firewall Services Module (FWSM) installed running version 2.3.1 or prior are affected when configured to allow exceptions for content filtering.

An example configuration of a filter exception which allows internal hosts to reach another network might be

```
FWSM#show filter
filter https except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter ftp except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter url except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter ftp 21 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter https 443 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

If the resulting output includes a **filter** command with an argument of **except**, you may be susceptible to the vulnerability outlined in this advisory.

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 No.
-----
 1 48 SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX SAxxxxxxxxxx
 4 6 Firewall Module WS-SVC-FWM-1 SAxxxxxxxxxx
 5 2 Supervisor Engine 720 (Active) WS-SUP720-BASE SAxxxxxxxxxx
 6 2 Supervisor Engine 720 (Hot) WS-SUP720-BASE SAxxxxxxxxxx
```

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 No.
-----
 4 6 Firewall Module WS-SVC-FWM-1 SAxxxxxxxxxx

Mod MAC addresses Hw Fw Sw Status
-----
 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.

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

```
FWSM#show version

FWSM Firewall Version 2.3(1)
```

For customers managing their FWSM via the PIX Device Manager (PDM), simply 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 window indicated by a label similar to:

FWSM Version: 2.3(1)

Products Confirmed Not Vulnerable

Products with similar functionality, such as the Cisco PIX Security Appliance and the Cisco Adaptive Security Appliance (ASA) 5500 Series, are not affected.

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

Details

The Cisco Firewall Services Module is a high-speed, integrated firewall module for Catalyst 6500 series switches and Cisco 7600 series routers. A vulnerability exists in the Cisco Firewall Services Module when configured for exceptions in content filtering in which inbound TCP packets can bypass access-list entries intended to explicitly filter them.

Although access lists (ACL) can be used to prevent outbound access to specific websites or File Transfer Protocol (FTP) servers via IP address and/or IP address/port pairs, configuring and managing web usage this way is often not practical because of the size and dynamic nature of the Internet. The FWSM may be used in conjunction with a Websense Enterprise or N2H2 server to better manage filtering of Hypertext Transfer Protocol (HTTP), HTTP over Secure Sockets Layer (HTTPS), and FTP connections to and from the Internet.

If URL, HTTPS, or FTP filtering exceptions has been configured via the command

filter < url | https | ftp > except

in order to exclude certain addresses from being filtered, then a vulnerability exists where any TCP traffic that matches this exception filter is also exempt from the inbound ACL inspection on any interface. Since filtering is enabled for outbound connections from the inside interface, a configuration may be common where any source address coming from an internal network is able to reach servers placed on a DMZ via a source address and mask of all zeros in order to simplify configurations.

An example configuration of a filter exception which allows internal hosts to reach another network might be:

```
FWSM# show filter
filter https except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter ftp except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter url except 0.0.0.0 0.0.0.0 10.1.3.0 255.255.255.0
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter ftp 21 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
filter https 443 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

In this example, all TCP traffic from any interface destined to hosts on the 10.1.3.0/24 network will bypass all FWSM interface input ACLs including those that explicitly deny them.

This vulnerability is documented as Cisco bug ID [CSCeh21590](#) ([registered](#) customers only).

Impact

Successful exploitation of the vulnerability may result in TCP traffic which would normally not be allowed past the FWSM on any interfaces to be able to reach hosts which should be protected by the FWSM.

Software Versions and Fixes

Cisco FWSM users can upgrade to version [2.3\(2\)](#) or later software to resolve this vulnerability. If older version of software is required, interim images are available from the TAC which also address this issue. Installations running 2.2 may upgrade to 2.2(1)18 or later and 1.1 users may upgrade to 1.1(4)4 or later.

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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") for assistance.

Workarounds

The effectiveness of any workaround 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 is the most appropriate for use in the intended network before it is deployed.

The workaround for this issue is to remove any filter exception rules which exist from the configuration. Filter exception rules would start with

```
filter < url | ftp | https > except
```

and may be removed using the **no** form of the command.

For more information on configuring the content filtering commands please consult:

<http://www.cisco.com/en/US/docs/security/fwsm/fwsm23/command/reference/df.html#wp1142003>

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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 assistance with the upgrade, which should be free of charge.

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

Please 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.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

See <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.

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>.

Exploitation and Public Announcements

The Cisco PSIRT has been made aware of an instance where a customer may have been impacted through the vulnerability described in this advisory.

This vulnerability was reported to Cisco by a customer.

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.

Distribution

This advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050511-url.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 (includes CERT/CC)
- bugtraq@securityfocus.com
- 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.

Revision History

Revision 1.0	2005-May-11	Initial public release.
--------------	-------------	-------------------------

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>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 11, 2005

Document ID: 64821
