

# Table of Contents

<u>Cisco Security Advisory: Cisco FWSM Vulnerabilities</u> .....	1
<u>Document ID: 47288</u> .....	1
<u>Revision 1.1</u> .....	1
<u>Last Updated 2003 December 17 at 1500 GMT</u> .....	1
<u>For Public Release 2003 December 15 at 1600 UTC (GMT)</u> .....	1
<u>Please provide your feedback on this document</u> .....	1
<u>Summary</u> .....	1
<u>Affected Products</u> .....	1
<u>Details</u> .....	2
<u>Impact</u> .....	2
<u>Software Versions and Fixes</u> .....	2
<u>Obtaining Fixed Software</u> .....	2
<u>Workarounds</u> .....	3
<u>Exploitation and Public Announcements</u> .....	4
<u>Status of This Notice: Final</u> .....	4
<u>Distribution</u> .....	4
<u>Revision History</u> .....	5
<u>Cisco Security Procedures</u> .....	5

# Cisco Security Advisory: Cisco FWSM Vulnerabilities

Document ID: 47288

## Revision 1.1

Last Updated 2003 December 17 at 1500 GMT

For Public Release 2003 December 15 at 1600 UTC (GMT)

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**Details**  
**Impact**  
**Software Versions and Fixes**  
**Obtaining Fixed Software**  
**Workarounds**  
**Exploitation and Public Announcements**  
**Status of This Notice: Final**  
**Distribution**  
**Revision History**  
**Cisco Security Procedures**

---

## Summary

This advisory documents two vulnerabilities for the Cisco Firewall Services Module for Cisco Catalyst 6500 Series and Cisco 7600 Series (FWSM). These vulnerabilities are documented as CSCeb16356 (HTTP Auth) and CSCeb88419 (SNMPv3).

There are workarounds available to mitigate the effects of CSCeb88419 (SNMPv3). No workaround is available for CSCeb16356 (HTTP Auth).

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20031215-fwsm.shtml>.

## Affected Products

All Cisco FWSM devices running the affected Cisco FWSM software, as documented below, are affected by these vulnerabilities.

- **CSCeb16356 (HTTP Auth)**  
1.1.2 and earlier.
- **CSCeb88419 (SNMPv3)**  
1.1.2 and earlier.

The Cisco PIX firewall is also vulnerable to the SNMPv3 issue and is documented as <http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.shtml>. No other Cisco products are currently known to be affected by these vulnerabilities.

To determine your software revision, type **show version** at the command line prompt.

## Details

- **CSCeb16356 (HTTP Auth)**

The Cisco FWSM may crash and reload due to a buffer overflow vulnerability while processing HTTP traffic requests for authentication using TACACS+ or RADIUS. This request is initiated when a user starting a connection via FTP, Telnet, or over the World Wide Web (HTTP) is prompted for their user name and password. If the user name and password are verified by the designated TACACS+ or RADIUS authentication server, the Cisco FWSM will allow further traffic between the authentication server and the connection to interact independently through the Cisco FWSM's "cut-through proxy" feature.

- **CSCeb88419 (SNMPv3)**

The Cisco FWSM crashes and reloads while processing a received SNMPv3 message when **snmp-server host <if\_name> <ip\_addr>** or **snmp-server host <if\_name> <ip\_addr> poll** is configured on the Cisco FWSM. This happens even though the Cisco FWSM does not support SNMPv3.

A Cisco FWSM configured to only generate and send traps using the **snmp-server host <if\_name> <ip\_addr> trap** command is not vulnerable.

The Internetworking Terms and Cisco Systems Acronyms online guides can be found at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/>.

These vulnerabilities are documented in the Cisco Bug Toolkit as Bug ID CSCeb16356 (HTTP Auth) and CSCeb88419 (SNMPv3). To access this tool, you must be a registered user and you must be logged in.

## Impact

- **CSCeb16356 (HTTP Auth)**

This vulnerability can be exploited to initiate a Denial of Service attack on the Cisco FWSM.

- **CSCeb88419 (SNMPv3)**

This vulnerability can be exploited to initiate a Denial of Service attack on the Cisco FWSM.

## Software Versions and Fixes

- **CSCeb16356 (HTTP Auth)**

1.1.3 and later.

- **CSCeb88419 (SNMPv3)**

1.1.3 and later.

The procedure to upgrade to the fixed software version is detailed at

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/fwsm/fwsm\\_1\\_1/fwsm112/admin.htm#wp104](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/fwsm/fwsm_1_1/fwsm112/admin.htm#wp104)

## Obtaining Fixed Software

Cisco is offering free software upgrades to address these vulnerabilities for all affected customers.

Cisco Security Advisory: Cisco FWSM Vulnerabilities

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 the Cisco Connection Online Software Center at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

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/tacpage/sw-center/lan/catalyst/crypto/>. To access the software download URL, you must be a registered user and you must be logged in.

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 obtaining the software upgrade(s).

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) using the contact information listed below. In these cases, customers are entitled to obtain an upgrade to a later version of the same release or as indicated by the applicable corrected software version in the Software Versions and Fixes section (noted above).

Cisco 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)

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.

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a upgrade. Upgrades for non-contract customers must be requested through the TAC.

Please do not contact either "[psirt@cisco.com](mailto:psirt@cisco.com)" or "[security-alert@cisco.com](mailto:security-alert@cisco.com)" for software upgrades.

## Workarounds

- **CSCeb16356 (HTTP Auth)**

No workaround. Please upgrade.

- **CSCeb88419 (SNMPv3)**

There are two workarounds available.

- ◆ If SNMP polling to the Cisco FWSM is required on a vulnerable image, one may choose to restrict the polling access to the SNMP server to trusted interfaces and trusted hosts by using this command:

```
snmp-server host <if_name> <ip_addr> poll
```

**Note:** *Both Poll and Trap are enabled if one does not specifically use the poll or trap keyword in the command above. The above command cannot prevent a source IP spoofed SNMP request message from exploiting this vulnerability.*

- ◆ Disable the SNMP server on the Cisco FWSM as follows:

```
clear snmp-server
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
```

**Note:** *The Cisco FWSM does not allow one to remove the community string altogether. It will always be either public or a user configured string. **show snmp** will still show **snmp-server community public**, but this does not mean SNMP is enabled.*

More details at

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_sw/v\\_62/cmdref/s.htm#wp1026423](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/cmdref/s.htm#wp1026423).

The Cisco PSIRT recommends that affected users upgrade to a fixed software version of code.

## Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

## Status of This Notice: Final

This is a final advisory. Although Cisco cannot guarantee the accuracy of all statements in this advisory, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this advisory.

**A stand-alone copy or paraphrase of the text of this security advisory 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-20031215-fwsm.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key having the fingerprint 8C82 5207 0CA9 ED40 1DD2 EE2A 7B31 A8CF 32B6 B590, 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) (includes CERT/CC)
- [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.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)
- Various internal Cisco mailing lists

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 1.1	2003–December–17	Added clear snmp-server command to the disable SNMP server workaround. Added elaborative text to the SNMPv3 details and workarounds sections.
Revision 1.0	2003–December–15	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](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>.

This advisory is copyright 2003 by Cisco Systems, Inc. This advisory may be redistributed freely after the release date given at the top of the text, provided that redistributed copies are complete and unmodified, including all date and version information.

---

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jul 05, 2005

Document ID: 47288

---