

Cisco Security Advisory: Cisco PIX Vulnerabilities

Document ID: 47284

Advisory ID: cisco-sa-20031215-pix

<http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.shtml>

Revision 1.2

Last Updated 2004 January 26 1600 UTC (GMT)

For Public Release 2003 December 15 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

This advisory documents two vulnerabilities for the Cisco PIX firewall. These vulnerabilities are documented as CSCeb20276 (SNMPv3) and CSCec20244 (VPNC).

There are workarounds available to mitigate the effects of CSCeb20276 (SNMPv3). No workaround is available for CSCec20244 (VPNC).

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

Affected Products

This section provides details on affected products.

Vulnerable Products

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

- CSCeb20276 (SNMPv3)

6.3.1, 6.2.2 and earlier, 6.1.4 and earlier. 5.x.x and earlier.

- **CSCec20244 (VPNC)**

6.2 (2.119) to 6.2.3, both inclusive.

6.3.x and 6.2.1 to 6.2 (2.118) are **not** affected.

The Firewall Service Module (FWSM) is also vulnerable to the SNMPv3 issue and is documented as <http://www.cisco.com/warp/public/707/cisco-sa-20031215-fwsm.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.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

This section provides detailed information about these vulnerabilities.

- **CSCeb20276 (SNMPv3)**

The Cisco PIX firewall 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 PIX firewall. This happens even though the Cisco PIX firewall does not support SNMPv3.

A Cisco PIX firewall configured to only generate and send traps using the **snmp-server host <if_name> <ip_addr> trap** command is not vulnerable.

- **CSCec20244 (VPNC)**

Under certain conditions an established VPNC IPsec tunnel connection is dropped if another IPsec client attempts to initiate an IKE Phase I negotiation to the outside interface of the VPN Client configured Cisco PIX firewall.

Only a Cisco PIX firewall configured as a VPN Client is vulnerable to this vulnerability. A device reload of the VPN Client configured PIX is required to recover from this unstable state. No action is required on the headend VPN concentrator.

A VPNC, also referred to as Easy VPN or ezVPN, connection is created when the Cisco PIX firewall is used as a VPN client to connect to a VPN server. An IKE Phase I negotiation is a step in the establishment of an IPsec session.

CSCec20244 resolved this issue for the 6.2 (3.100) and later software releases.

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 CSCeb20276 (SNMPv3) and CSCec20244 (VPNC). To access this tool, you must be a [registered](#) user and you must be logged in.

Impact

This section describes the impact of the issues described in this document.

- **CSCeb20276 (SNMPv3)**

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

- **CSCec20244 (VPNC)**

This vulnerability can be exploited to initiate a Denial of Service attack on sessions established between a Cisco PIX configured as a VPN Client and a VPN server.

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.

- **CSCeb20276 (SNMPv3)**
6.3.2 and later, 6.2.3 and later, 6.1.5 and later.
- **CSCec20244 (VPNC)**
6.3.1 and later, 6.2(3.100) and later.

The procedure to upgrade to the fixed software version is detailed at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/index.htm.

Workarounds

This section describes workarounds for these vulnerabilities.

- **CSCeb20276 (SNMPv3)**
There are two workarounds available.
 - If SNMP polling to the PIX 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. Prior to software version 6.0, one cannot selectively enable poll and trap functionality because there are no **Poll** and **Trap** keywords in the **snmp-server host <if_name> <ip addr>** command.*

– Disable the SNMP server on the Cisco PIX firewall 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 PIX firewall 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/en/US/docs/security/pix/pix62/command/reference/s.html#wp1026423>.

- **CSCec20244 (VPNC)**
No workaround. Please upgrade.

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

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 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 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.

Exploitation and Public Announcements

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

CSCeb20276 (SNMPv3) was reported to the PSIRT by Rasto Rickardt.

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-20031215-pix.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
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- 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 1.2	2004-January-26	Removed reference to CSCea28896, as it did not affect any released software. Added elaborative text to the SNMPv3 workaround section.
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. 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.

[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: Jan 26, 2004

Document ID: 47284
