[NEWS] Cisco PIX Vulnerabilities (SNMP, VPNC)

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2003−12/0062.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 12/18/03

```
To: list@securiteam.com
Date: 18 Dec 2003 16:49:31 +0200
```

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: http://www.securiteam.com
− − promotion

The SecuriTeam alerts list − Free, Accurate, Independent.

Get your security news from a reliable source.
http://www.securiteam.com/mailinglist.html

− − − − − − − − −

Cisco PIX Vulnerabilities (SNMP, VPNC)
−−−

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:
 * 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/CSCea28896 (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 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.

CSCea28896 resolved this issue for the 6.3.x software releases and 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/> 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/CSCea28896 (VPNC). To access this tool, you must be a registered user and you must be logged in.

Impact:
 * CSCeb20276 (SNMPv3)
This vulnerability can be exploited to initiate a Denial of Service attack on the Cisco PIX firewall.

 * CSCec20244/CSCea28896 (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:
 * CSCeb20276 (SNMPv3) 6.3.2 and later, 6.2.3 and later, 6.1.5 and later.

 * CSCec20244/CSCea28896 (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>
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/index.htm.

Workarounds:
 * CSCeb20276 (SNMPv3)

There are two workarounds available.
 o 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.

 o 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/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/s.htm#1026423>
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/cmdref/s.htm#1026423.

 * CSCec20244/CSCea28896 (VPNC)

No workaround. Please upgrade.

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

ADDITIONAL INFORMATION

The information has been provided by <mailto:psirt@cisco.com> Cisco
Systems Product Security Incident Response Team.

==========

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list−unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list−subscribe@securiteam.com

==========
==========

DISCLAIMER:
The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.