

[NEWS] Cisco Pix Firewall DoS (NAT Pool Depletion)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0014.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/07/03

To: list@securiteam.com

Date: 7 Oct 2003 16:07:44 +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/maillinglist.html>

Cisco Pix Firewall DoS (NAT Pool Depletion)

SUMMARY

Users of Cisco Pix Firewalls may discover that their pool of NAT'ed IP addresses is running out, and that a reboot or reload of the firewall clears the problem, this is due to a vulnerability in the Cisco Pix Firewall that allows specially constructed ICMP packets to deplete the pool.

DETAILS

Vulnerable Systems:

* Cisco Pix Firewall IOS versions 6.2.2 and 6.3.(3.102)

The problem is caused by the Firewall being swamped by incoming ICMP packets on the global pool IP addresses. If these are not intercepted by a router beforehand, the incoming echo requests (that are emanating from Nachi/Welchia worm infected machines) are preventing the release of the address translation. i.e.: The Cisco Pix Firewall is detecting the blocked traffic as indication that the translation is still in use.

Workaround:

Securiteam: [NEWS] Cisco Pix Firewall DoS (NAT Pool Depletion)

For those who are unable to block incoming ICMP echo requests at their router (for whatever reason), Cisco has released the following details:

- 1 – use PAT (a global pool with a single entry) this way although the xlate will remain up but all your internal hosts will be multiplexed over this pat address. single pat address can accommodate in theory 65535 connections. However, this might break un-PATable traffic
- 2 – Use statics for your important servers that need NAT (1 to 1 mapping)
- 3 – Also instead of rebooting the whole pix you can simply log into it and do "clear xlate" this will clear all translations.</I<

It should be pointed out that "2" is not a solution to this problem. The others are not ideal either.

Vendor Status:

Cisco was notified and bug ID CSCec47609 has been opened to investigate this issue.

Cisco have updated the Security Notice about the "Nachi Worm Mitigation Recommendations" (

<<http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sn-20030820-nachi.shtml>) to reflect this information.

ADDITIONAL INFORMATION

The information has been provided by <mailto:John.Airey@rnib.org.uk> John Airey

=====

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.