

Cisco Security Notice: Response to Full-Disclosure – Potential Denial of Service Bug in Cisco Pix Firewall IOS 6.2.2 and 6.3.(3.102)

Document ID: 59663

Revision 1.0

Last Updated 2005 July 25

Please provide your feedback on this document.

[Summary](#)
[Details](#)
[Cisco Security Procedures](#)

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report: <http://lists.netsys.com/pipermail/full-disclosure/2003-October/011356.html> . Cisco responded with the following, which is also archived at <http://lists.netsys.com/pipermail/full-disclosure/2003-October/011379.html> .

```
To: Full-Disclosure
Subject: Re: Potential denial of service bug in Cisco Pix Firewall IOS 6.2.2 and 6.3.(3.102)
Date: Fri, 03 Oct 2003 20:21:14 +0200
Author: Ilker Temir <itemir@cisco.com>
In-Reply-To: <John.Airey@rnib.org.uk>
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

```
This is in response to the e-mail posted by John Airey. The original
e-mail is available at
```

```
http://lists.netsys.com/pipermail/full-disclosure/2003-October/011356.html
```

```
Hi John,
```

```
Cisco's Product Security Incident Response Team (PSIRT) was not
previously aware of this issue. Thank you for bringing it to our attention.
```

```
Cisco bug ID CSCec47609 has been opened to investigate this issue. We
have updated the Security Notice about the "Nachi Worm Mitigation
```

Recommendations"

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

We are always open for vulnerability reports regarding any Cisco products. Such reports can be directly sent to us at psirt@cisco.com or to security-alert@cisco.com in case of an emergency.

Best regards,

Ilker

John.Airey@rnib.org.uk wrote:

| Brief Description

| -----

| Users of Cisco Pix Firewalls may discover that their pool of NAT'ted IP
| addresses is running out, and that a reboot or reload of the firewall
clears
| the problem.

| Details

| -----

| 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. ie, the Pix is detecting the blocked traffic as
| indication that the translation is still in use.

| I believe that this bug also affects the recent security update version
| 6.3(3.102) detailed at

[www.cisco.com/en/US/tech/tk583/tk618/technologies_security_advisory09186a008
| 01c5975.shtml](http://www.cisco.com/en/US/tech/tk583/tk618/technologies_security_advisory09186a00801c5975.shtml).

| I have been unable (and unwilling) to test this, but given that a
permanent

| fix is being worked on it is undoubtedly the case.

| Workaround

| -----

| For those who are unable to block incoming ICMP echo requests at their
| router (for whatever reason), Cisco have sent me 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 accomodate 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."

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

| Permanent fix

| -----

I have been informed that Cisco are aware of this and that a bug fix is being worked on.

Other

I am releasing this notification as there may well be system administrators who are still suffering from this problem. Specifically the release of this information cannot lead to any further attacks against systems that are already affected.

Unfortunately Cisco have not updated their information regarding mitigation against the Nachi/Welchia worm at

www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a00801b143a.shtml

The mitigation information only covers outgoing connections. I have asked Cisco for a fix to for this twice, and at present I am still waiting for a resolution to my second request.

Apologies for the evil Outlook word-wrapping, which may render URLs above useless.

Please be kind to me. This is my first security vulnerability I've ever posted.

-

John Airey, BSc (Jt Hons), CNA, RHCE
Internet systems support officer, ITCSD, Royal National Institute of the Blind,
Bakewell Road, Peterborough PE2 6XU,
Tel.: +44 (0) 1733 375299 Fax: +44 (0) 1733 370848 John.Airey@rnib.org.uk

Our world is intolerant, and always will be. We kid ourselves when we think that those who have different values can tolerate each other.

-

DISCLAIMER:

NOTICE: The information contained in this email and any attachments is confidential and may be privileged. If you are not the intended recipient you should not use, disclose, distribute or copy any of the content of it or of any attachment; you are requested to notify the sender immediately of your receipt of the email and then to delete it and any attachments from your system.

RNIB endeavours to ensure that emails and any attachments generated by its staff are free from viruses or other contaminants. However, it cannot accept any responsibility for any such which are transmitted. We therefore recommend you scan all attachments.

Please note that the statements and views expressed in this email and any attachments are those of the author and do not necessarily represent those of RNIB.

RNIB Registered Charity Number: 226227

Website: <http://www.rnib.org.uk>

```
| Full-Disclosure - We believe in it.  
| Charter: http://lists.netsys.com/full-disclosure-charter.html  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.2.1 (GNU/Linux)  
  
iD8DBQE/fb4Z8/wE0ppYtwURAgW4AJ9aqTn9EKSkckykitdhrLcDFVV2mwCcDJty  
2zYqJsoln8xkt0VikUllr6c=  
=hKKK  
-----END PGP SIGNATURE-----
```

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: Jul 25, 2005

Document ID: 59663
