

Cisco Security Response: Cisco PIX embryonic state machine TTL(n-1) DoS and Cisco PIX embryonic state machine 1b data DoS

Document ID: 69335

<http://www.cisco.com/warp/public/707/cisco-sr-20060307-pix.sh>

Revision 1.0

For Public Release 2006 March 07 2030 UTC (GMT)

Please provide your feedback on this document.

Cisco Response
Additional Information
Revision History
Cisco Security Procedures

Cisco Response

This is Cisco PSIRT's response to the statements made by Arhont Ltd.– Information Security in their messages [Full-disclosure] Cisco PIX embryonic state machine TTL(n-1) DoS and [Full-disclosure] Cisco PIX embryonic state machine 1b data DoS, both posted on March 7, 2006.

The original emails are available at
<http://lists.grok.org.uk/pipermail/full-disclosure/2006-March/042771.html> and
<http://lists.grok.org.uk/pipermail/full-disclosure/2006-March/042772.html>.

These issues have the same root cause that was documented in Arhont Ltd.– Information Security's message [Full-disclosure] Cisco PIX TCP Connection Prevention, posted on November 22, 2005, at
<http://lists.grok.org.uk/pipermail/full-disclosure/2005-November/038971.html>.

As detailed in our reply also dated November 22, 2005, this issue is being tracked by two Cisco Bug IDs:

- **CSCsc14915** — PIX 6.3 Spoofed TCP SYN packets can block legitimate TCP connections
This Bug ID tracks the issue for PIX software version 6.3 and older. This DDTS is resolved and available in PIX software version 6.3(5.106). There are workarounds available to mitigate the issue.
- **CSCsc16014** — PIX 7.0 Spoofed TCP SYN packets can block legitimate TCP connections
This Bug ID tracks the issue for PIX/ASA software version 7.0. This DDTS is resolved and available in PIX/ASA software versions 7.0(4.005) and 7.1(1). Additional mitigations and workarounds exist to limit or eliminate the issue.

Our November 22, 2005, reply is available at
<http://www.cisco.com/warp/public/707/cisco-response-20051122-pix.shtml>.

We would like to thank Arhont Ltd.– Information Security for ensuring that these issues were previously addressed as well.

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

Additional Information

There have been updates to the information available for these two Bug IDs since November 22, 2005. The updated Release Note Enclosures are available at:

- **CSCsc14915** --- PIX 6.3 Spoofed TCP SYN packets can block legitimate TCP connections
<http://www.cisco.com/pcgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc14915> (registered customers only)
- **CSCsc16014** --- PIX 7.0 Spoofed TCP SYN packets can block legitimate TCP connections
<http://www.cisco.com/pcgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc16014> (registered customers only)

Revision History

Revision 1.0	2006-March-07	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>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 07, 2006

Document ID: 69335
