

Cisco Security Response: Response to PIX/ASA/FWSM Websense/N2H2 Content Filter Bypass

Document ID: 70090

<http://www.cisco.com/warp/public/707/cisco-sr-20060508-pix.shtml>

Revision 1.0

For Public Release 2006 May 08 1700 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 George Gal in his advisory: WebSense Content Filter Bypass in conjunction with Cisco PIX in packet filter mode, posted on May 08, 2006.

The original email/advisory is available at
<http://www.vsecurity.com/bulletins/advisories/2006/cisco-websense-bypass.txt> .

This issue is being tracked by Cisco Bug IDs:

- [CSCsc67612](#) ([registered](#) customers only) — Fragmented HTTP Request Websense URL Filtering Bypass Pix 6.3.x
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(112). Now workarounds exist to eliminate this issue.
- [CSCsc68472](#) ([registered](#) customers only) — Fragmented HTTP Request Websense URL Filtering Bypass PIX/ASA 7.x
This Bug ID tracks the issue for PIX/ASA software version 7.x. This DDTS is resolved and available in PIX/ASA software versions 7.0(5)and 7.1(2). No workarounds exist to eliminate this issue.
- [CSCsd81734](#) ([registered](#) customers only) — Segmented HTTP request bypasses Websense/N2H2 URL filtering
This Bug ID tracks the issue for FWSM software version 2.3 and 3.1. This DDTS is resolved and available in FWSM software versions 2.3(4)and 3.1(1.7). No workarounds exist to eliminate this issue.

We would like to thank George Gal of Virtual Security Research for reporting this issue to us.

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

If various PIX/ASA/FWSM software versions are configured to use Websense/N2H2 for content filtering, users may be able to bypass HTTP content restrictions. By fragmenting the GET method of an HTTP request into multiple packets, it is possible to cause a condition in which the PIX/ASA/FWSM firewall will mistakenly allow a restricted website to be accessed. The PIX/ASA/FWSM firewall expects the entire GET method to be received in one packet. There are no workarounds which mitigate or eliminate this issue.

PIX software version 6.3.5(112) and later resolves this issue. Interim releases of PIX 6.3 software are only available by contacting the Cisco TAC or your Cisco support partner. Please reference this security response when requesting software to ensure the proper software version is obtained.

PIX/ASA software versions 7.0(5) and 7.1(2) resolve this issue. Maintenance releases of PIX/ASA 7.x software may be downloaded at the following sites.

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix?psrtdcat20e2>

<http://www.cisco.com/cgi-bin/tablebuild.pl/asa?psrtdcat20e2>

FWSM software versions 2.3(4), 3.1(1.7) and later resolve this issue. FWSM software version 2.3(4) may be downloaded at the following site.

<http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm?psrtdcat20e2>

Interim releases of FWSM 3.1 software are only available by contacting the Cisco TAC or your Cisco support partner. Please reference this security response when requesting software to ensure the proper software version is obtained.

Revision History

1.0	2006-May-08	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/warp/public/707/sec_incident_response.shtml. 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: May 08, 2006

Document ID: 70090
