

Cisco Security Response: WebVPN Cross-Site Scripting Vulnerability

Document ID: 70469

<http://www.cisco.com/warp/public/707/cisco-sr-20060613-webvpn-xss.shtml>

Revision 1.0

For Public Release 2006 June 13 2200 UTC (GMT)

Please provide your [feedback](#) on this document.

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the response of the Cisco Product Security Incident Response Team (PSIRT) to the statements made by Michal Zalewski <lcamtuf@dione.ids.pl> in his message entitled "SSL VPNs and security", which he posted to the Bugtraq and full-disclosure mailing lists on June 8, 2006.

The original emails are available at <http://www.securityfocus.com/archive/1/436479/30/0/threaded> (Bugtraq archive) and at <http://archives.neohapsis.com/archives/fulldisclosure/2006-06/0094.html> (full-disclosure archive).

In his posting to Bugtraq and full-disclosure, Michal Zalewski mentions a Cross-Site Scripting (XSS) vulnerability that exists in "Cisco SSL VPN."

Cisco confirms the existence of an XSS vulnerability in the clientless mode of the WebVPN feature of the Cisco VPN 3000 Series Concentrators and the Cisco ASA 5500 Series Adaptive Security Appliances (ASA).

Please note that the technology affected by the XSS vulnerability covered in Michal Zalewski's message is what Cisco calls "WebVPN clientless mode" and not "WebVPN full-network-access mode", which is a different encrypted tunnel technology that is more similar to IPsec and that requires the installation of the Cisco SSL VPN Client.

For a description of the differences between the clientless and full-network-access modes of Cisco WebVPN please refer to:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6657/product_data_sheet0900aecd80405e25.html

Cisco is tracking this issue using the following Cisco bug IDs:

- [CSCsd81095](#) ([registered](#) customers only) – VPN3k vulnerable to cross-site scripting when using WebVPN
- [CSCse48193](#) ([registered](#) customers only) – ASA vulnerable to cross-site scripting when using WebVPN

Additional Information

The vulnerability happens when certain error conditions occur and the device tries to make the user aware of the problem. Under these error conditions the WebVPN feature presents the user with an HTML page that indicates the error and the URL the user was trying to access.

Because the pages displayed also output the URL that caused the problem, it is possible to embed scripting code in the URL that then will be executed by the user's web browser.

In his posting to Bugtraq and full-disclosure, Michal Zalewski provides the example "https://<vpnhost>/webvpn/dnserror.html?domain=<u>foo</u>". In this example, the vulnerability is triggered when the device displays a DNS resolution problem ("dnserror.html"). The other possible page where this problem can happen is "connecterror.html", which is displayed when the device has trouble connecting to the URL specified by the user.

Cisco bugs [CSCsd81095](#) ([registered](#) customers only) and [CSCse48193](#) ([registered](#) customers only) will address the issue for all WebVPN error conditions.

To exploit these issues an attacker would have to entice authenticated users to follow a specially crafted, malicious URL. A successful attack would result in the execution of arbitrary script code in the user's web browser.

As Michal Zalewski points out, SSL VPN technologies have their own set of challenges. The whitepaper on SSL VPN Security that is mentioned in the original posting to Bugtraq and full-disclosure is a good resource on this topic that attempts to address the nature of these challenges and increase awareness. This whitepaper is located at:

http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html

This issue was independently reported to Cisco by Michal Zalewski and two other customers. We would like to thank them for bringing this issue to our attention.

Revision History

Revision 1.0	2006 June 13	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>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)
