

# Cisco Security Response: Cross-Site Scripting Vulnerability in Online Help System

Document ID: 82421

<http://www.cisco.com/warp/public/707/cisco-sr-20070315-xss.shtml>

## Revision 1.2

Last Updated 2007 April 11 1430 UTC (GMT)

For Public Release 2007 March 15 1700 UTC (GMT)

---

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

---

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

---

## Cisco Response

A cross-site scripting (XSS) vulnerability in the online help system distributed with several Cisco products has been independently reported to Cisco by Erwin Paternotte from Fox-IT and by Cassio Goldschmidt.

The vulnerability would allow an attacker to execute arbitrary scripting code in a user's web browser if the attacker is successful in enticing the user to follow a specially crafted, malicious URL.

Multiple Cisco products are affected because the vulnerable online help system is used by several Cisco products.

This response is posted at <http://www.cisco.com/warp/public/707/cisco-sr-20070315-xss.shtml>

## Additional Information

The vulnerability exists specifically in the content search feature of the online help system. This feature allows the user to search for specific keywords in the help contents. The search feature is implemented through an HTML form and scripting code.

The vulnerability exists because the search code in the file *PreSearch.html* (or in the file *PreSearch.class*, depending of the product) fails to properly sanitize all of the user's input.

The vulnerability is triggered when a search keyword that includes scripting code enclosed by `<script>` and `</script>` tags is entered in the text field of the search form. In some cases, the initial text is sanitized, but further text is not, so scripting code after the initial text can also trigger the vulnerability. For example: "some text `<script>alert('I am a script')</script>`".

User intervention is required for an attacker to be able to successfully exploit this vulnerability: an attacker must be able to trick a user into following a malicious, specially crafted, URL. In some cases, the user must be

authenticated to the web interface offered by the product for management or regular use.

The following Cisco products are affected by this vulnerability (all versions are affected unless a specific version is explicitly mentioned):

- Cisco Secure Access Control Server (ACS) for Windows and Cisco Secure ACS Solution Engine. All 4.x versions are affected. Versions prior to 4.0 are not affected. Cisco Bug ID [CSCsh91761](#) ([registered customers only](#)) .
- Cisco VPN Client. Cisco Bug ID [CSCsh52300](#) ([registered customers only](#)) .
- Cisco Unified Personal Communicator. Cisco Bug ID [CSCsh91884](#) ([registered customers only](#)) .
- Cisco MeetingPlace and Cisco Unified MeetingPlace, end-user and Admin help systems. Cisco Bug ID [CSCsi12435](#) ([registered customers only](#)) .
- Cisco Unified MeetingPlace Express, end-user and Admin help systems. Cisco Bug ID [CSCsh91901](#) ([registered customers only](#)) .
- Cisco CallManager. Cisco Bug ID [CSCsi10405](#) ([registered customers only](#)) .
- Cisco IP Communicator. Cisco Bug ID [CSCsh91953](#) ([registered customers only](#)) .
- Cisco Unified Video Advantage (formerly Cisco VT Advantage). Cisco Bug ID [CSCsh93070](#) ([registered customers only](#)) .
- Cisco Unified Videoconferencing 3545 System, Cisco Unified Videoconferencing 3540 Series Videoconferencing System, Cisco Unified Videoconferencing 3515 MCU, Cisco Unified Videoconferencing 3527 PRI Gateway, Cisco Unified Videoconferencing 3526 PRI Videoconferencing Gateway, and Cisco Unified Videoconferencing Manager. Cisco Bug ID [CSCsh93854](#) ([registered customers only](#)) .
- Cisco WAN Manager (CWM). Cisco Bug ID [CSCek71039](#) ([registered customers only](#)) .
- Cisco Security Device Manager. Cisco Bug ID [CSCsh95009](#) ([registered customers only](#)) .
- Cisco Network Analysis Module (WS-SVC-NAM-1 and WS-SVC-NAM-2) for Catalyst 6500 series switches and Cisco 7600 series routers. Cisco Bug ID [CSCsi10818](#) ([registered customers only](#)) .
- Cisco Network Analysis Module (NM-NAM) for modular access routers (Cisco 26xx, 26xxXM, 28xx, 36xx, 37xx, 38xx). Cisco Bug ID [CSCsi10818](#) ([registered customers only](#)) .
- CiscoWorks and all products that integrate with CiscoWorks. Cisco Bug ID [CSCsi10674](#) ([registered customers only](#)) .

Affected CiscoWorks-related products include:

- ◆ Management Center for IPS Sensors
- ◆ Security Monitor
- ◆ CiscoWorks LAN Management Solution
- ◆ Router Management Essentials
- ◆ Common Services
- ◆ Device Fault Manager
- ◆ CiscoView

- ◆ Internetwork Performance Monitor (IPM)
- ◆ Campus Manager
- Cisco Wireless LAN Solution Engine (WLSE). Cisco Bug ID [CSCsi10982](#) ([registered](#) customers only) .
- Cisco 2006 Wireless LAN Controllers (WLC). Cisco Bug ID [CSCsi13743](#) ([registered](#) customers only) .
- Cisco Wireless Control System (WCS). Cisco Bug ID [CSCsi13763](#) ([registered](#) customers only) .
- VPN 3000 Series Concentrators. Cisco Bug ID [CSCsi47620](#) ([registered](#) customers only) .

In some cases it is possible to eliminate the vulnerability by removing or renaming the files *PreSearch.html* and *PreSearch.class* (if they exist – use your operating system's file search feature to locate them.) Please note that this workaround is not applicable to appliances and other products where direct access to the file system is not available, and that by removing or renaming these files it will no longer be possible to search the product's online help contents.

For additional information on Cross-Site Scripting (XSS) attacks and the methods used to exploit these vulnerabilities, please refer to the Cisco Applied Mitigation Bulletin "Understanding Cross-Site Scripting (XSS) Threat Vectors", available at:

<http://www.cisco.com/warp/public/707/cisco-amb-20060922-understanding-xss.shtml>

The Cisco PSIRT is not aware of any malicious use of the vulnerability described in this document.

This issue was independently reported to Cisco by Erwin Paternotte from Fox-IT and by Cassio Goldschmidt. The original reports were for the Cisco CallManager and for the Cisco VPN Client, respectively. Further investigation revealed a number of additional affected products. We would like to thank Erwin Paternotte, Fox-IT, and Cassio Goldschmidt for bringing this issue to our attention and for working with us towards coordinated disclosure of the issue.

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

## Revision History

Revision 1.2	2007-April-11	Added the VPN 3000 Series Concentrators as an affected product.
Revision 1.1	2007-March-23	Version 4.0.x of Cisco Secure Access Control Server (ACS) for Windows and Cisco Secure ACS Solution Engine is also affected (the original release of this document incorrectly stated that only version 4.1 was affected.)  Clarify that it is the Network Analysis Module

		(WS-SVC-NAM-1, WS-SVC-NAM-2, and NM-NAM) what is affected, and not the operating system (IOS or CatOS) of the device the module is inserted into.
Revision 1.0	2007-March-15	Initial public release in coordination with Erwin Paternotte from Fox-IT and with Cassio Goldschmidt.

## 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](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: Apr 11, 2007

Document ID: 82421

---