

Cisco Security Response: Cisco Secure ACS for UNIX Cross Site Scripting Vulnerability

Document ID: 70471

<http://www.cisco.com/warp/public/707/cisco-sr-20060615-acs.shtml>

Revision 1.0

For Public Release 2006 June 15 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 response to the statements made by Fujitsu Services Limited in their advisory, posted on June 15, 2006 to several external mailing lists.

This vulnerability is addressed by Cisco Bug ID:

- [CSCsd50560](#) ([registered](#) customers only) ACS LogonProxy.cgi vulnerable to Cross Site Scripting attacks.

We would like to thank Thomas Liam Romanis and Fujitsu Services Limited for reporting this vulnerability 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

Cisco Secure Access Control Server (ACS) is a centralized user access control framework. Cisco Secure ACS offers centralized command and control for all user authentication, authorization, and accounting (AAA pronounced "triple A") services to network devices that function as AAA clients.

Cisco Secure ACS for UNIX LogonProxy.cgi is vulnerable to Cross Site Scripting (XSS) attacks via both HTML GET and POST requests.

This vulnerability affects only Cisco Secure ACS for Unix.

Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine are not affected.

This vulnerability could be used to redirect the ACS administrative users to another host which could be used to proxy login requests back to the bona fide ACS server while harvesting administrative user credentials.

Solution

Download and apply patch for CSCsd50560, which is located on Cisco.com at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cspatchunix-3des>.

Instructions for applying the patch are found at the same location.

The following best practices will help mitigate the risks of this vulnerability:

- Ensure that only IP addresses of trusted administrator hosts can access the Cisco Secure ACS server.
- Prevent access to the web component of the ACS server over the Internet.

Revision History

Revision 1.0	2006-June-15	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](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 15, 2006

Document ID: 70471
