

Table of Contents

<u>Cisco Security Notice: Response to BugTraq – Cisco Secure ACS Cross Site Scripting Issue</u>	1
<u>Revision 1.0</u>	1
<u>Last Updated 2002 June 21</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Cisco Security Procedures</u>	2

Cisco Security Notice: Response to BugTraq – Cisco Secure ACS Cross Site Scripting Issue

Revision 1.0

Last Updated 2002 June 21

Please provide your feedback on this document.

Summary
Details
Cisco Security Procedures

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report: <http://www.securityfocus.com/archive/1/277053> . Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/278222> .

```
To: BugTraq
Subject: Re: XSS in CiscoSecure ACS v3.0
Date: Jun 21 2002 2:15AM
Author: Lisa Napier <lnapier@cisco.com>
Message-ID: <4.3.2.7.2.20020620143404.027e5618@twoguys>
In-Reply-To: <20020614203944.35711.qmail@web9503.mail.yahoo.com>
```

Hi Dave,

Thank you for posting this information. The defect ID's for Cisco customers who wish to track this issue via the Cisco Bug toolkit on our website are: CSCdx88709 and CSCdx88715 for both affected release versions.

Thank you,

Lisa Napier
Product Security Incident Response Team
Cisco Systems

```
At 01:39 PM 6/14/2002, Dave Palumbo wrote:
>sMax. Security Advisory
>-----
>
>Title: Cross-Site Scripting in CiscoSecure ACS v3.0
>Date: June 14, 2002
```

```
>
>PRODUCT AFFECTED:
>
>CiscoSecure ACS v3.0 (Win32)
>
>PRODUCT OVERVIEW:
>
>CiscoSecure ACS is Cisco's implementation of RADIUS.
>v3.0 is the current release of the product. Taken
>from their website: "Cisco Secure ACS provides
>authentication, authorization, and accounting
>(AAA pronounced "triple A") services to network
>devices that function as AAA clients, such as a
>network access server, PIX Firewall, or router."
>
>VULNERABILITY:
>
>Testing CiscoSecure ACS v3.0(1), Build 40 reveals a
>cross-site scripting problem in the web server
>component. Specifically, the "action" argument that
>the setup.exe handler uses does not appear to do
>proper input validation. Other arguments were not
>tested, though they may be vulnerable as well.
>
>Proof-of-concept:
>http://IP.ADD.RE.SS:dyn_port/setup.exe?action=<script>alert('foo+bar')</script>&page=list.
>(URL may wrap)
>
>Obviously one needs to already be authenticated to the
>ACS web server for this to successfully be carried
>out.
>
>SOLUTION:
>
>Follow best practices, don't make the web component of
>ACS server available over the Internet.
>
>Cisco was contacted on May 21st. They have committed
>to fixing this in the next release of the software,
>due out in "mid to late summer".
>
>- Dave Palumbo
>
>
>_____
>Do You Yahoo!?
>Yahoo! - Official partner of 2002 FIFA World Cup
>http://fifaworldcup.yahoo.com
```

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>.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.