

# Cisco Security Response: Cisco Secure ACS Denial Of Service Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20080903-csaacs.shtml>

## Revision 1.0

For Public Release 2008 September 03 1600 UTC (GMT)

---

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

---

## Contents

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

---

## Cisco Response

This is the Cisco PSIRT response to the statements made by Laurent Butti and Gabriel Campana of Orange Labs / France Telecom Group, in their advisory: "Cisco Secure ACS EAP Parsing Vulnerability". The original advisory is available at:

<http://www.securityfocus.com/archive/1/495937/30/0/threaded> 

A specially crafted Remote Authentication Dial In User Service (RADIUS) Extensible Authentication Protocol (EAP) Message Attribute packet sent to the Cisco Secure Access Control Server (ACS) can crash the CSRadius and CSAuth processes of Cisco Secure ACS. Because this affects CSAuth all authentication requests via RADIUS or TACACS+ will be affected during exploitation of this vulnerability.

Cisco ACS installations that are configured with AAA Clients to authenticate using TACACS+ only are not affected by this vulnerability.


The RADIUS shared secret and a valid known Network Access Server (NAS) IP address must be known to carry out this exploit.


The Cisco PSIRT team greatly appreciates the opportunity to work with researchers on security vulnerabilities, and we welcome the opportunity to review and assist in product reports. We thank Laurent Butti and Gabriel Campana of Orange Labs / France Telecom Group for reporting this vulnerability to Cisco PSIRT.

Software patches are available for customers with support contracts and should be obtained through their regular support channels. The upgrade to fixed software is not a free upgrade. See Software Versions and Fixes section within this advisory for further information on obtaining fixed software.

## Additional Information

Cisco Secure ACS provides a comprehensive, identity-based access control solution for Cisco intelligent information networks. It is the integration and control layer for managing enterprise network users, administrators, and the resources of the network infrastructure.

Described in [RFC2865](#) , RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server (Cisco Secure ACS) that contains all user authentication and network service access information.

Described in [RFC3748](#) , EAP is an authentication framework that supports multiple authentication methods. Typically, EAP runs directly over data link layers, such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP.

All versions of Cisco Secure ACS for Windows (ACS) and the Cisco Secure ACS Solution Engine (ACSE) prior to the fixed software versions listed in this Response are affected by this vulnerability. Cisco Secure ACS Express, Cisco Secure for Unix and Cisco Access Register are not affected by this vulnerability.

A specially crafted RADIUS EAP Message Attribute packet will crash the CSRADIUS and CSAUTH services. An error message will be indicated in the Windows event viewer - System Log indicating "The CSAUTH service terminated unexpectedly" and "The CSRADIUS service terminated unexpectedly". In the Cisco ACS **Reports and Activity** tab, under **ACS Service Monitoring**, the logs will indicate CSAUTH is not running and attempts to restart.

The CSRADIUS service handles communication between the service for authentication and authorization (CSAUTH service) and the access device requesting the authentication and authorization services for RADIUS.

Continued exploitation of this vulnerability will prevent Cisco Secure ACS from processing all authentication and authorization requests via RADIUS or TACACS+. In many cases continued exploitation will prevent network access to devices which first require authentication or authorization via the AAA Server.

This vulnerability is documented in Cisco bug ID [CSCsq10103](#) ([registered](#) customers only) and Common Vulnerabilities and Exposures (CVE) identifier [CVE-2008-2441](#) has been assigned to this vulnerability.

## Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Affected Release	First Fixed Release
3.X.Y	Release 3.3(4) Build 12 patch 8 or later
4.0.X	Vulnerable; Contact TAC
4.1.X	Release 4.1(4) Build 13 Patch 11 or later
4.2.X	Release 4.2(0) Build 124 Patch 4 or later

The fixed software for Cisco Secure ACS for Windows (ACS) can be downloaded from: <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des>

The fixed software for Cisco Secure ACS Solution Engine (ACSE) can be downloaded from: <http://www.cisco.com/cgi-bin/tablebuild.pl/acs-soleng-3des?psrtdcat20e2>

The first fixed release files names are indicated below:

	3.x cumulative patch	4.1 cumulative patch	4.2 cumulative patch
<b>CS ACS for Windows</b>	Acs-3.3.4.12.8-SW.zip	Acs-4.1.4.13.11-SW.zip	ACS-4.2.0.124.4-SW.zip
<b>CS ACS Solution Engine</b>	applAcs-3.3.4.12.7.zip	applAcs_4.1.4.13.11.zip	applAcs_4.2.0.124.4.zip

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 1.0	2008-September-03	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](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>.

---

### Help us help you.

#### Please rate this document.

- Excellent  
 Good  
 Average  
 Fair  
 Poor

#### This document solved my problem.

- Yes  
 No  
 Just browsing

#### Suggestions for improvement:

(256 character limit)

Send

[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

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