

# [NEWS] Cisco Secure Access Control Server (ACS) Multiple DoS and Authentication Vulnerabilities

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0098.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 08/30/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 30 Aug 2004 16:46:48 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Cisco Secure Access Control Server (ACS) Multiple DoS and Authentication Vulnerabilities

---

## SUMMARY

<<http://www.cisco.com/en/US/products/sw/secursw/ps2086/>> Cisco Secure Access Control Server "for Windows (ACS Windows) and Cisco Secure Access Control Server Solution Engine (ACS Solution Engine) provide authentication, authorization, and accounting (AAA) services to network devices such as a network access server, Cisco PIX and a router".

This advisory documents multiple Denial of Service (DoS) and authentication related vulnerabilities for the ACS Windows and the ACS Solution Engine servers.

## DETAILS

Vulnerable Systems:

- \* Cisco Secure ACS versions 3.2(3) and earlier are vulnerable to CSCef05950 and CSCed81716
- \* Cisco Secure ACS version 3.2(2) build 15 is vulnerable to CSCeb60017
- \* Cisco Secure ACS version 3.2 is vulnerable to CSCec90317 and CSCec66913
- \* Cisco Secure ACS is vulnerable to CSCed81716

## Securiteam: [NEWS] Cisco Secure Access Control Server (ACS) Multiple DoS and Authentication Vulnerabilities

Immune Systems:

- \* Cisco Secure ACS for UNIX

Note: Successfully authenticate to your ACS box to determine your software revision. After you perform the authentication, the first screen displays the current ACS version in this format–CiscoSecure ACS Release 3.2(3) Build 11. ACS versions may also be displayed as 003.002(003.011), where "011" is the build number referenced on the ACS graphical user interface (GUI).

The vulnerabilities mentioned above are described in better detail in the following paragraphs:

- \* CSCeb60017 and CSCec66913 – Cisco Secure ACS provides a Web-based management interface, termed CSAdmin, which listens on TCP port 2002. When flooded with TCP connections the ACS Windows and ACS Solution Engine stops responding to any new TCP connections destined for port 2002.

Additionally, services on the ACS that process authentication related requests might become unstable and stop responding, which hampers the ability for ACS to process any authentication related requests. A reboot of the device is required to restore these services.

- \* CSCec90317 – Cisco Secure ACS, when configured for Light Extensible Authentication Protocol (LEAP) RADIUS Proxy, forwards LEAP authentication requests to a secondary RADIUS server. The ACS device with LEAP RADIUS proxy configured may crash when LEAP authentication requests are being processed. A reboot is required to bring the device back to an operational state.

- \* CSCed81716 – Cisco Secure ACS can communicate with external databases and authenticate users against those databases. One of the external databases that ACS supports is Novell Directory Services (NDS). If an anonymous bind in NDS is allowed, and if the ACS Solution Engine is authenticating NDS users with NDS as the external database and not Generic LDAP, then users are able to authenticate with blank passwords against that NDS database. However, wrong passwords and incorrect usernames are properly rejected.

- \* CSCef05950 – Once a user successfully authenticates to the ACS GUI on TCP port 2002, a separate TCP connection is created between the browser and ACS administration Web service, with a random destination port. If an attacker spoofs the IP address of the user computer, and accesses the ACS GUI on this random port, then the attacker may be able to connect to the ACS GUI, bypassing authentication. Authentication to the ACS server may also be bypassed if the attacker is behind the same PAT device as that of the ACS user and accesses the ACS GUI on this random port.

Impact

- \* CSCeb60017, CSCec66913, and CSCec90317 – These vulnerabilities may cause a crash impacting the availability of services on the ACS devices. Until the device is rebooted a DoS is the result.

## Securiteam: [NEWS] Cisco Secure Access Control Server (ACS) Multiple DoS and Authentication Vulnerabilities

\* CSCed81716 – This vulnerability may allow unauthorized users to access AAA clients without an effective password (using blank passwords) if the bind to the NDS database is anonymous.

\* CSCef05950 – This vulnerability may allow unauthenticated users to gain access to the ACS Administration GUI.

### Patch Availability:

The above mentioned vulnerabilities have already been fixed by Cisco.

Users are encouraged to perform upgrade procedures, as indicated:

\* ACS Windows version 3.3 –

<[http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod\\_installation\\_guide09186a0080238b18.html#wp9989](http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080238b18.html#wp9989)>  
[http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod\\_installation\\_guide09186a0080238b18.html#wp9989](http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080238b18.html#wp9989)

\* ACS Windows 3.2 –

<[http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod\\_installation\\_guide09186a0080184928.html#wp9472](http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080184928.html#wp9472)>  
[http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod\\_installation\\_guide09186a0080184928.html#wp9472](http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080184928.html#wp9472)

\* ACS Solution Engine –

<[http://www.cisco.com/en/US/products/sw/secursw/ps5338/products\\_user\\_guide\\_chapter09186a0080204d45.html#wp9472](http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_user_guide_chapter09186a0080204d45.html#wp9472)>  
[http://www.cisco.com/en/US/products/sw/secursw/ps5338/products\\_user\\_guide\\_chapter09186a0080204d45.html#wp9472](http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_user_guide_chapter09186a0080204d45.html#wp9472)

### Possible Workarounds:

\* Configure an IP address filter on ACS Windows and ACS Solution Engine to limit the exposure of these vulnerabilities. From within the ACS GUI, browse to Administration Control > Access Policy to limit access to only the machines that need to administer the ACS remotely.

\* Apply access control lists (ACLs) on routers, switches and firewalls that filter traffic to the ACS so that traffic is only allowed from stations that need to remotely administer the box. Refer to <<http://www.cisco.com/warp/public/707/tacl.html>>  
<http://www.cisco.com/warp/public/707/tacl.html> for examples on how to apply ACLs on Cisco routers.

\* As a best practice, use HTTPS to limit access to the Cisco ACS GUI. Issues detailed in CSCef05950 still exist when you use HTTP instead of HTTPS to access the Cisco ACS GUI.

### Refer to

<[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/acs32/user02/a.htm#wp89030](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/user02/a.htm#wp89030)>  
[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/csacs4nt/acs32/user02/a.htm#wp89030](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/user02/a.htm#wp89030) for information on how to set up an access policy on the Cisco ACS.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@cisco.com>> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20040825-acis.shtml>>  
<http://www.cisco.com/warp/public/707/cisco-sa-20040825-acis.shtml>

Securiteam: [NEWS] Cisco Secure Access Control Server (ACS) Multiple DoS and Authentication Vulnerabilities

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.