

Cisco Security Response: Cisco Secure ACS Weak Session Management Vulnerability

Document ID: 70553

<http://www.cisco.com/warp/public/707/cisco-sr-20060623-acs.shtml>

Revision 1.2

Last Updated 2006 July 03 1300 UTC (GMT)

For Public Release 2006 June 23 2200 UTC (GMT)

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

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to the statements made by Darren Bounds in his advisory: Cisco Secure ACS Weak Session Management Vulnerability. The original email/advisory is available at

<http://www.securityfocus.com/archive/1/438161>

and

<http://lists.grok.org.uk/pipermail/full-disclosure/2006-June/047301.html>

The attacks described in the report take advantage of a weakness in the default configuration of the Cisco Secure Access Control Server (ACS).

These issues are being tracked by the following Cisco ID numbers (registered customers only)

- [CSCse26754](#) ([registered](#) customers only) ACS/ACSE Administration may do limited session validation.
- [CSCse63433](#) ([registered](#) customers only) ACS Unix "Fast Admin" may do limited session validation.
- [CSCse26719](#) ([registered](#) customers only) Cisco Secure Port Redirect may be predictable.

Cisco PSIRT will update this security response on an "as-needed" basis as additional information on these issues become available.

Additional Information

The following vulnerability affects Cisco Secure ACS for Windows (ACS), the Cisco Secure ACS Solution Engine (ACSE) and Cisco Secure ACS for Unix (CSU). Versions 4.0 and earlier of Cisco Secure ACS and Cisco Secure ACS Solution Engine are affected by this vulnerability. Versions 2.3.6 and earlier of Cisco Secure ACS for Unix are affected by this vulnerability.

The vulnerability is tracked with two different Cisco IDs, for the different platforms.

- [CSCse26754](#) ([registered](#) customers only) ACS/ACSE Administration may do limited session validation.

Once authenticated, ACS and ACSE perform remote client administrator session validation based on the source IP address of the client administrative host.

If the administrative user has authenticated itself to the Cisco Secure server and started a session on the default administration login port (2002/tcp), the session will be redirected to another TCP port selected by the server. By spoofing the IP address belonging to the administrative client host in use by the user to connect to the Cisco Secure interface, an attacker might be able to take over the administrative session without being prompted for authentication credentials.

ACS and ACSE are affected by this vulnerability only when an active authenticated administrator session is already in place.

- [CSCse63433](#) ([registered](#) customers only) ACS Unix "Fast Admin" may do limited session validation.

The "Fast Admin" portion of Cisco Secure ACS for UNIX performs remote client administrator session validation based on the source IP address of the client administrative session. In the event that an administrator has already authenticated with the Cisco Secure ACS for UNIX and has not entered into "Advanced Admin" portion, it is possible by spoofing the source IP client address to gain access to the Cisco Secure administrative session, without further being prompted for user credentials.

The "Advanced Admin" portion of CSU is not vulnerable to this issue.

Cisco Secure ACS for UNIX is affected by this vulnerability only when an active authenticated "Fast Admin" administrator session is already in place.

The following vulnerability affects only Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine. Versions 4.0 and earlier for Cisco Secure ACS and Cisco Secure ACS Solution Engine are affected by this vulnerability. Cisco Secure for Unix is NOT affected by this vulnerability:

- [CSCse26719](#) ([registered](#) customers only) Cisco Secure Port Redirect may be predictable.

ACS and ACSE perform port redirection from the default administration login port of 2002/tcp to the allocated authorized administrative session port, in two different ways depending on the configuration of the Cisco Secure ACS server:

If "HTTP Port Allocation" within 'Administration Control --> Access Policy' is configured to "Allow any TCP ports to be used for Administration HTTP Access", the behavior is allocation of the next sequential available port number, within the operating system and is fairly predictable.

If the HTTP port allocation is set to "Restrict Administration Sessions to the following port range", the port allocated is a random number in the specified port range and hence not predictable in the manner described above.

Workarounds

The following mitigations/workarounds should be deployed to mitigate the risks associated with the described vulnerabilities.

Cisco Secure ACS for Unix

In order to mitigate the risks associated with this vulnerability on Cisco Secure ACS for UNIX, Cisco recommends restricting the source IP address to trusted subnets and deploying anti-spoofing techniques:

- Ensure that only IP addresses of trusted administrator hosts can access the Cisco Secure ACS server.

1. Edit the \$BASEDIR/config/CSConfig.ini file and set ValidateClients = true.
2. Ensure that valid source IP addresses are entered of the trusted hosts that will be allowed to access the ACS server.
3. Stop the CiscoSecure process using \$BASEDIR/utills/kcs
4. Start the CiscoSecure process using \$BASEDIR/utills/scs

The following sample configuration illustrates the deployment of restricting source IP address to a single trusted client:

```
[ValidClients]
100 = 192.168.10.10
; Add list of trusted clients above ^^^ in the format:
; ClientID = Client's Host Name
; CGI stub's clientID=100, and it's host name
; For example 100 = localhost or 100 = 192.92.182.2
; 101 = 192.92.190.5
;
;if ValidateClients=true, then we only allow the clients with ids listed
;above to connect to the dbserver
ValidateClients = true
```

For additional information on the use of the "ValidClients" configuration option, please see http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/cs_unx/acsu235/app_b.htm#wp1015734.

- Ensure that only IP addresses of trusted administrator hosts can access the FastAdmin portion of Cisco Secure ACS for UNIX.
1. Edit the \$BASEDIR/config/CSConfig.ini file and set FastAdminValidateClients = true.
 2. Ensure that valid source IP addresses are entered of the trusted hosts that will be allowed to access the FastAdmin portion of the Cisco Secure ACS for Unix server.
 3. Stop the CiscoSecure process using \$BASEDIR/utills/kcs
 4. Start the CiscoSecure process using \$BASEDIR/utills/scs

The following sample configuration illustrates the deployment of restricting access to the FastAdmin portion of Cisco Secure for Unix to a single trusted client:

```
[ValidClients]
.
[lines removed]
.
;if FastAdminValidateClients = true, then we only allow the clients with ids listed
;below to connect to the FastAdmin 100 = 192.168.10.10 FastAdminValidateClients = tr
```

Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine

For Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine to help mitigate the risks of these vulnerabilities, Cisco recommends that customers deploy the following mitigations by using the HTTP GUI:

- Within 'Administration Control --> Access Policy' Cisco Secure ACS administrative screen:
 - "IP Address Filtering" settings.

Configure "Allow only listed IP addresses to connect" to restrict the valid source IP address of administrative clients that may access the Cisco Secure ACS server. Restrict access to the web

interface to only trusted client IP address or subnets.

- "HTTP Configuration" settings.

Configure "Restrict Administration Sessions to the following port range" to "From Port 1024 to Port 65535". This forces Cisco Secure ACS to use its own randomized port redirection algorithm which is not predictable compared with the default port redirection setting of "Allow any TCP ports to be used for Administration HTTP Access". This is a workaround to the disclosed vulnerability.

- "Secure Socket Layer Setup"

Use HTTPS for all remote Cisco Secure ACS administrative sessions. This increases the difficulty in gaining unauthorized access to or control over an authenticated ACS administrative session. ACS only allows you to enable SSL for administrative sessions after you have installed a server certificate and a certification authority certificate on the 'ACS Certificate Setup page' in 'System Configuration'

- Within 'Administration Control --> Session Policy' Cisco Secure ACS administrative screen:

- Set "Session idle timeout" for administrative sessions to a suitable time period.

The default for the number of minutes of inactivity within the administrative session is 60 minutes. Once this time-out has been reached, the browser terminates the remote administration connection, after which a new session would require re-authentication.

- Respond to invalid IP address connections

By default this check box is selected and Cisco Secure ACS will respond with an error message to the remote administrator when the workstation is on an invalid, unauthorized IP address range for remote access. If this check box is cleared, no error message is generated when an invalid remote connection attempt is made. Administrators can disable this option to prevent unauthorized identification of ACS.

To prevent spoofed IP packets with the source IP address set to that of the Cisco Secure ACS administrative management station from reaching the Cisco Secure ACS server, utilize anti-spoofing techniques. For more information on utilizing ACLs for anti-spoofing, refer to <http://www.cisco.com/warp/public/707/21.pdf> and <http://www.ietf.org/rfc/rfc2827.txt>.

The Unicast Reverse Path Forwarding (Unicast RPF) feature helps to mitigate problems that are caused by forged IP source addresses that are passing through a router. Refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf/scfrpf.htm for more information.

Revision History

Revision 1.2	2006–July–03	Updated Workaround/Cisco Secure ACS for Unix section with additional information.
Revision 1.1	2006–June–28	Added new Cisco Bug ID (CSCse63433) to Cisco response section. Content added to Additional Information section.

Revision 1.0	2006 June 23	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](#) © 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 03, 2006

Document ID: 70553
