

Cisco Security Response: Response to Symantec SYMSA-2006-003 Cisco Secure ACS for Windows – Administrator Password Disclosure

Document ID: 70091

<http://www.cisco.com/warp/public/707/cisco-sr-20060508-acs.shtml>

Revision 1.0

For Public Release 2006 May 08 2145 UTC (GMT)

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

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

Cisco Response

This is Cisco PSIRT's response to the statements made by Symantec in its advisory: SYMSA-2006-003, posted on May 8, 2006.

The original email/advisory is available at
<http://www.symantec.com/enterprise/research/SYMSA-2006-003.txt>.

This issue is being tracked by Cisco Bug ID:

- [CSCsb67457](#) ([registered](#) customers only) — Cisco Secure ACS Administrator Password Remote Retrieval and Decryption.

We would like to thank Andreas Junestam and Symantec 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) provides centralized identity management and policy enforcement for Cisco devices.

[CSCsb67457](#) ([registered](#) customers only) — Cisco Secure ACS Administrator Password Remote Retrieval and Decryption.

Symptom:

A person with administrative access to the Windows registry of a system running Cisco Secure ACS 3.x for Windows can decrypt the passwords of all ACS administrators.

Condition:

Cisco Secure ACS 3.x for Windows stores the passwords of ACS administrators in the Windows registry in an encrypted format. A locally generated master key is used to encrypt/decrypt the ACS administrator passwords. The master key is also stored in the Windows registry in an encrypted format. Using Microsoft cryptographic routines, it is possible for a user with administrative privileges to a system running Cisco Secure ACS to obtain the clear-text version of the master key. With the master key, the user can decrypt and obtain the clear-text passwords for all ACS administrators. With administrative credentials to Cisco Secure ACS, it is possible to change the password for any locally defined users. This may be used to gain access to network devices configured to use Cisco Secure ACS for authentication.

If remote registry access is enabled on a system running Cisco Secure ACS, it is possible for a user with administrative privileges (typically domain administrators) to exploit this vulnerability.

If Cisco Secure ACS is configured to use an external authentication service such as Windows Active Directory / Domains or LDAP, the passwords for users stored by those services are not at risk to compromise via this vulnerability.

This vulnerability only affects version 3.x of Cisco Secure ACS for Windows. Cisco Secure ACS for Windows 4.0.1 and Cisco Secure ACS for UNIX are not vulnerable. Cisco Secure ACS 3.x appliances do not permit local or remote Windows registry access and are not vulnerable.

Workaround:

It is possible to mitigate this vulnerability by restricting access to the registry key containing the ACS administrators' passwords. One feature of Windows operating systems is the ability to modify the permissions of a registry key to remove access even for local or domain administrators. Using this feature, the registry key containing the ACS administrators' passwords can be restricted to only the Windows users with a need to maintain the ACS installation or operate the ACS services.

The following registry key and all of its sub-keys need to be protected.

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv3.3\CSAdmin\Administrators

Note: The "CiscoAAAv3.3" portion of the registry key path may differ slightly depending on the version of Cisco Secure ACS for Windows that is installed.

There are two general deployment scenarios for Cisco Secure ACS. The Windows users that need permissions to the registry key will depend on the deployment type.

- If Cisco Secure ACS is not installed on a Windows domain controller, access to the registry key should be limited to only the local Windows SYSTEM account and specific local/domain administrators who will be performing software maintenance on the ACS installation.
- If Cisco Secure ACS is installed on a Windows domain controller, access to the registry key should be limited to the domain account which ACS is configured to use for its services, the local Windows SYSTEM account and specific local / domain administrators who will be performing software maintenance on the ACS installation.

For information about editing the Windows registry, please consult the following Microsoft documentation.

"Description of the Microsoft Windows registry":

<http://support.microsoft.com/default.aspx?scid=kb:EN-US:256986>

Further mitigation against remote exploitation can be achieved by restricting access to authorized users or disabling remote access to the Windows registry on systems running Cisco Secure ACS for Windows. For information on restricting remote registry access, please consult the following Microsoft documentation.

"How to restrict access to the registry from a remote computer":

<http://support.microsoft.com/kb/q153183>

"How to Manage Remote Access to the Registry":

<http://support.microsoft.com/kb/q314837>

Revision History

Revision 1.0	2006 May 08	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/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>.

[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: May 08, 2006

Document ID: 70091
