

[NT] Cisco Secure ACS Web Server Found to Contain Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0009.html>

From: support@securiteam.com

Date: 04/04/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 4 Apr 2002 10:46:34 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Cisco Secure ACS Web Server Found to Contain Vulnerabilities

SUMMARY

Cisco Secure Access Control Server (ACS) for Windows contains two vulnerabilities. One vulnerability can lead to the execution of an arbitrary code on an ACS server and the second can lead to an unauthorized disclosure of information. The patch is available for both vulnerabilities.

Cisco Secure ACS for UNIX is not vulnerable. No other Cisco product is vulnerable.

There is no direct workaround for the vulnerabilities but it is possible to mitigate them largely. See the Workarounds section for details.

DETAILS

Affected Products:

The affected product is Cisco Secure Access Control Server for Windows releases 2.6.x and ACS 3.0.1 (build 40). A patch is available.

Cisco Secure ACS for UNIX is not affected.

Securiteam: [NT] Cisco Secure ACS Web Server Found to Contain Vulnerabilities

No other Cisco products are affected.

Details:

There are two different vulnerabilities, as described by the Bug IDs below. The first can lead to execution of an arbitrary code; the second can be used to reveal customer data.

Bug IDs CSCdx17622 and CSCdx17683

By connecting to port 2002 and sending a crafted URL, it is possible to, in a less severe case, kill the CSADMIN module or, in a severe case, to execute an arbitrary user-supplied code. The functionality of authentication, authorization, and accounting (AAA) is not affected by termination of the CSADMIN module. This means that users will be able to authenticate normally. Only the administration function will be affected. Port 2002 is used by the CSADMIN module for remote administration.

By providing a URL containing formatting symbols (for example, %s, %p), it is possible to execute a user-provided code.

Bug IDs CSCdx17689 and CSCdx17698

By using "..\" in the URL it is possible to access data in any directory outside the Web root directory but on the same hard disk or disk partition. With this technique, it is possible to access only the following file types: html, htm, class, jpg, jpeg, or gif.

Please note that an attacker must know the exact location and file name. It is not possible to browse a directory this way.

Impact:

By exploiting the format vulnerability, an attacker may execute arbitrary code on the machine. This code will be executed in the same context as the CSADMIN process, and that is as administrator. Executing arbitrary code will lead to a total compromise of the machine.

By exploiting the directory traversal vulnerability, an attacker can gain unauthorized access to information in the following file types: html, htm, class, jpg, jpeg, or gif. The main issue may be html files with hard coded passwords or other sensitive information.

Software Versions and Fixes:

Both vulnerabilities are fixed by the patched CSAdmin.exe files available at <<http://www.cisco.com/cgi-bin/tablebuild.pl/cs-acs-win>> <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-acs-win>. The file names are CSAdmin-patch-2.6-4-4.zip and CSAdmin-patch-3.0-1-40.zip.

Note: To download these patches, you must be a registered user and you must be logged in. Unregistered users should refer to the instructions in the Obtaining Fixed Software section.

To install the patch, follow the procedure below while logged in as Administrator.

Securiteam: [NT] Cisco Secure ACS Web Server Found to Contain Vulnerabilities

- 1) Manually stop the CSAdmin service.
- 2) Rename the <ACS-DIR>/CSAdmin/CSAdmin.exe file
- 3) Copy the patched CSAdmin.exe to <ACS-DIR>/CSAdmin.
- 4) Manually start the CSAdmin service.

Obtaining Fixed Software:

Cisco is offering a free software patch to address this vulnerability for all affected customers. Customers may only install and expect support for the feature sets they have purchased.

Customers with service contracts should contact their regular update channels to obtain any software release containing the feature sets they have purchased. For most customers with service contracts, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Web site at <<http://www.cisco.com>> <http://www.cisco.com>.

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for assistance with the upgrade.

Customers who purchased directly from Cisco but who do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale, should obtain fixed software by contacting the Cisco Technical Assistance Center (TAC). In these cases, customers may only upgrade to a later version of the same release.

Cisco TAC contacts are as follows:

- * +1 800 553 2447 (toll-free from within North America)
- * +1 408 526 7209 (toll call from anywhere in the world)
- * e-mail: tac@cisco.com

See <<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>> <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Please have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Workarounds:

There are no direct workarounds for these vulnerabilities. However, by exercising the standard best practices, it is possible to significantly mitigate both issues. These practices are:

Securiteam: [NT] Cisco Secure ACS Web Server Found to Contain Vulnerabilities

* Block all unnecessary traffic on the outer network edge. This includes private IP address space (10.0.0.0, for example) and spoofed packets. This can be accomplished using routers or firewalls. For instruction on how to accomplish this with Cisco routers, please consult documents at <<http://www.cisco.com/public/cons/isp/>> <http://www.cisco.com/public/cons/isp/>.

* Separate critical internal infrastructure from the rest of your internal network.

We strongly recommend that these practices are also followed when deploying Cisco ACS for Unix, even though it is not vulnerable to the mentioned issues.

ADDITIONAL INFORMATION

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

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Remote Buffer Overflow Vulnerability in IRIX SNMP Daemon"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)