

Cisco Security Advisory: Web Interface Vulnerabilities in Cisco Secure ACS for Windows

Document ID: 22167

Advisory ID: cisco-sa-20020403-acs-win-web

<http://www.cisco.com/warp/public/707/cisco-sa-20020403-acs-win-web.shtml>

Revision 1.1

Last Updated 2002 April 05 1600 UTC (GMT)

For Public Release 2002 April 03 1600 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

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. A 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 to a great extent. See the [Workarounds](#) section for details.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20020403-acs-win-web.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The affected product is Cisco Secure Access Control Server for Windows; all releases up to and including 2.6.x and ACS 3.0.1 (build 40) are affected.

Products Confirmed Not Vulnerable

Cisco Secure ACS for Unix is not affected.

No other Cisco products are currently known to be affected by these vulnerabilities.

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. This technique is described in the following article:
<http://www.securityfocus.com/archive/1/66842> .
- **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 hardcoded 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-acis-win> . The file names are **CSAdmin-patch-2.6-4-4.zip** and **CSAdmin-patch-3.0-1-40.zip**. These patches must be applied only to releases 2.6(4.4) and 3.0.1 (build 40). If you are running any other release, you should [open a case with the Cisco Technical Assistance Center \(TAC\)](#) to receive a free upgrade. After upgrading to release 2.6(4.4) or 3.0.1 (build 40), you should apply the patches.

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.

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.

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:

- 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/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml.
- 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.

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

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

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

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 guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct 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 get their upgrades by contacting the Cisco Technical Assistance Center (TAC). 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

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <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.

Exploitation and Public Announcements

Both vulnerabilities were reported by Jonas Ländin and Patrik Karlsson from iXsecurity. Cisco PSIRT was made aware that an exploit program for the format vulnerability exists. This exploit is not thought to be released to the general public.

Status of This Notice: FINAL

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.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020403-acs-win-web.shtml>. In addition to Worldwide Web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to

check the above URL for any updates.

Revision History

Revision 1.1	2002–April–05	Updates made to Affected Products, and Software Versions and Fixes.
Revision 1.0	2002–April–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 Web site 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](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 05, 2002

Document ID: 22167
