

Cisco Security Advisory: Cisco Secure ACS Unix Acme.server Information Disclosure Vulnerability

Document ID: 24981

Advisory ID: cisco-sa-20020702-acsunix-acmeweb

<http://www.cisco.com/warp/public/707/cisco-sa-20020702-acsunix-acmeweb>.

Revision 1.2

Last Updated 2002 July 24 0100 UTC (GMT)

For Public Release 2002 July 2 1800 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 for Unix implements the Acme.server and is therefore vulnerable to a directory traversal vulnerability. The fix has been included in ACS Unix version 2.3.6.1 which is currently available.

This vulnerability is detailed in Cisco Bug ID CSCdu47965.

This advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20020702-acsunix-acmeweb.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The defects described in this document are present in releases beginning with version 2.0 up to and including version 2.3.6 of Cisco Secure ACS for Unix Server.

Products Confirmed Not Vulnerable

Cisco Secure ACS for Windows NT is *not* vulnerable to this issue. Cisco Access Registrar is *not* vulnerable to this issue.

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

Details

This vulnerability exists within the Acme.server program that is part of the Cisco Secure ACS Unix installation. This vulnerability has been repaired in the Acme.server utility. The patch is available for Cisco customers, and has now been incorporated into the Cisco Secure ACS Unix product.

The vulnerability is triggered when someone browses to the server URL and adds trailing slashes as in the following example: `http://servername:9090///`. This exploit will display the files and filesystem of the target server.

This vulnerability has been assigned Cisco bug ID CSCdu47965.

Impact

The impact may vary, depending whether potential attackers have access to port 9090 on the Cisco Secure ACS computer. This vulnerability could allow an attacker to view files and directory structures on the target system. Access to the encrypted password file provided by this vulnerability, for example, would allow an attacker access through a successful dictionary attack against the listed accounts.

Customers who may have been vulnerable to attack are advised to review privileged accounts and any suspicious database changes, and to change administrative passwords.

Software Versions and Fixes

There is a patch available, and the fixes are included in Cisco Secure ACS Unix version 2.3.6.1 and all versions going forward. For existing versions, the patch may be applied, which resolves the issue. There is no need to upgrade to a newer version.

Workarounds

Workarounds for this vulnerability include general recommendations of protecting the Cisco Secure ACS for Unix with strong firewalls, access controls, and preventing any external or unauthenticated access to the system, and to port 9090 in particular. This is an interim workaround only, and a patch or upgrade is recommended.

For this issue, a patch is available which may be installed in place of an upgrade. The patch is available at the following temporary location:

`ftp://ftpeng.cisco.com/ftp/csu/Acme-Patch.tar.Z`

For any assistance with the patch, please contact the TAC. This patch fixes the security problem with the Acme.server. It includes the modified files provided by Acme. This patch can be applied for any supported version of Cisco Secure, that is, CiscoSecure/Unix 2.3(3) or later. The patch consists of one file: FastAdmin/Acme.zip.

Patch Installation Instructions

To install the patch, follow the instructions below. The commands need to be executed on your Cisco Secure ACS Unix by the administrator.

1. Stop Cisco Secure by entering the command:

```
/etc/rc0.d/K80CiscoSecure
```

2. Change to the base directory where Cisco Secure is installed.

```
cd $BASEDIR
```

3. Copy the compressed tar file Acme-Patch.tar.Z into the current directory.
4. Uncompress and untar the file.

```
uncompress Acme-Patch.tar.Z
tar xvf Acme-Patch.tar
```

5. Start Cisco Secure with the command:

```
/etc/rc2.d/S80CiscoSecure
```

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

The issue with the Acme.server was posted to the Bugtraq list June 2001 , although no specific mention of the Cisco product was made in the original posting. Cisco PSIRT is not aware of any malicious use of the vulnerability described in this advisory.

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 the Cisco worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20020702-acsunix-acmeweb.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 1.2	2002-July-24	Update to Affected Products section
Revision 1.1	2002-July-03	Update to Workarounds section
Revision 1.0	2002-July-02	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>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 24, 2002

Document ID: 24981
