

Cisco Security Advisory: CiscoSecure Access Control Server for UNIX Remote Administration Vulnerability

Document ID: 13654

Advisory ID: cisco-sa-19990819-dbaccess

<http://www.cisco.com/warp/public/707/cisco-sa-19990819-dbaccess.shtml>

Revision 1.0

For Public Release 1999 August 19 1500 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

In CiscoSecure Access Control Server (CiscoSecure ACS) for UNIX, versions 1.0 through 2.3.2, there is a database access protocol that could permit unauthorized remote users to read and write the server database without authentication. Depending on the network environment, this might permit unauthorized users to modify the access policies enforced by the CiscoSecure ACS. A utility that is capable of using this protocol to read or modify a database is shipped with the CiscoSecure ACS product.

This vulnerability can be eliminated by either a CiscoSecure configuration change, or network configuration change. Cisco has provided a new release that changed a default setting, in order to ensure higher default security level.

This vulnerability has Cisco bug ID CSCdm71489.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-19990819-dbaccess.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

If you are running an affected version of CiscoSecure ACS for UNIX, and if you have not modified the configuration to strictly permit connections from trusted hosts, and if untrusted users can make TCP connections to TCP port 9900 on the computer on which you have installed CiscoSecure ACS, then you are vulnerable.

Products Confirmed Not Vulnerable

Users of CiscoSecure ACS for Windows NT are *not* vulnerable.

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

Details

This vulnerability has been assigned Cisco bug ID CSCdm71489.

Impact

The impact may vary, depending whether potential attackers have access to port 9900 on the CiscoSecure ACS computer. This vulnerability could allow an attacker to remove accounts, add accounts and change passwords or privileges in the user database, including implementing an administrative account, that would give them control of the CiscoSecure ACS server.

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

Software Versions and Fixes

This applies **ONLY** to CiscoSecure ACS for UNIX, and is present in all versions, up to version 2.3.2. Version 2.3.3 of CiscoSecure ACS for UNIX has been modified to validate administrative clients by default.

This vulnerability applies only to the software product CiscoSecure Access Control Server for UNIX, and does not apply to CiscoSecure Access Control Server for NT.

Workarounds

Two workarounds for this vulnerability exist.

One workaround consists of enabling client validation within CiscoSecure ACS for UNIX. A caveat to this workaround is that there are some versions of CiscoSecure ACS for UNIX that are subject to another defect, which prevents access to additional administration utilities (the Advanced Administration GUI) within CiscoSecure ACS for UNIX when the client validation feature is enabled. This problem is identified in CSCdm72555 which affects versions 2.3.1 and 2.3.2, and CSCdk55423, which affects versions 2.2.2, 2.2.3 of CiscoSecure ACS for UNIX. This workaround will not be effective in CiscoSecure ACS for UNIX version

2.2.2, 2.2.3, 2.3.1 and 2.3.2, and customers are encouraged to upgrade to a version that does not include this defect. Version 2.3.3 is currently available and is not susceptible to the above problem.

You must edit the CSCconfig.ini file, list the permitted remote access hosts, enable remote client validation. TACACS or RADIUS clients do NOT need to be listed under this setting, only hosts that are permitted to administer the server should be listed.

In the following example, 'acs_srv_machine' resolves to localhost, and we are providing remote administration privileges to the hosts 'client_machine' and the ip address 172.16.23.23. Permitted clients may be defined by a hostname, or an ip address.

CSCconfig.ini file should be edited with the following information:

```
[ValidClients]

;if ValidateClients=true, than we only allow the clients with ids listed

; to connect to the dbserver

100 = acs_srv_machine

100 = client_machine

100 = 172.16.23.23

ValidateClients = true

...
```

An additional configuration parameter "FastAdminValidClients" was added in CiscoSecure ACS version 2.3.3 allowing the Fast Administrator Web based GUI to permit the same IP addresses specified in the valid clients list, to further restrict client access.

A second workaround is to use filtering on other network devices, such as a firewall, to control or block access to TCP port 9900 on the CiscoSecure ACS for UNIX server.

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

Cisco does not have any reports of malicious use of this vulnerability. CiscoSecure ACS for UNIX Reference Guide does include a cautionary note regarding this vulnerability.

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-19990819-dbaccess.shtml>. In addition to Worldwide Web

Cisco Security Advisory: CiscoSecure Access Control Server for UNIX Remote Administration Vulnerability

posting, the initial version of this notice is being sent 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
- first-info@first.org
- Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's Worldwide Web server, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the URL given above for any updates.

Revision History

Revision 1.0	1999-August-19	Initial public release.
--------------	----------------	-------------------------

Cisco Security Procedures

Cisco's Worldwide Web site contains complete information for reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information directly from Cisco at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices.

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

Updated: Aug 19, 1999

Document ID: 13654
