

Cisco Security Advisory: Cisco Secure Access Control Server Novell Directory Service Expired/Disabled User Authentication Vulnerability

Document ID: 22198

Advisory ID: cisco-sa-20020207-acs-nds-auth

<http://www.cisco.com/warp/public/707/cisco-sa-20020207-acs-nds-auth.shtml>

Revision 1.0

For Public Release 2002 February 07 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

Specific versions of Cisco Secure Authentication Control Server (ACS) allows authentication of users that have been explicitly disabled or expired in the Novell Directory Services (NDS). There is a software patch that may be applied, and software upgrades will also address this problem.

The complete notice will be available at
<http://www.cisco.com/warp/public/707/cisco-sa-20020207-acs-nds-auth.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

Only Cisco Secure ACS version 3.0.1, configured for NDS, is affected.

Products Confirmed Not Vulnerable

The following are NOT affected by this vulnerability:

- Systems with Cisco Secure ACS for Windows NT version 2.6 and 2.5 and earlier
- Cisco Secure ACS version 3.0.1 that is NOT configured for use with NDS
- Cisco Secure ACS for UNIX

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

Details

To determine if your Cisco Secure ACS for Windows NT server is configured for NDS, please review the "External User Databases/Unknown User Policy" on the Administration interface. If the name of your NDS configuration appears in the "Selected Databases" list, then you are using NDS for authentication and are affected by this vulnerability if you are running version 3.0.1.

Users who are marked as "expired" or "disabled" on the NDS database will still authenticate if their credentials are otherwise correct. The file "NDSAuth.DLL" is a module which allows ACS authentication to be handled by an external NDS server. Versions of this file with the date 2001-Dec-15 ignore the "Disabled" or "Expired" state of these users on NDS. Authentication attempts by users with a Disabled or Expired status on the NDS server should be refused, but are permitted due to this vulnerability.

This vulnerability is documented in Cisco Bug ID CSCdw46931.

- **CSCdw46931** — DEL/ACS authenticates NDS expired/disabled users.

Impact

This vulnerability results in a failure to adequately enforce authentication criteria, and users that should be prevented from using services are permitted to authenticate, regardless of their status in the NDS server.

Software Versions and Fixes

CiscoSecure ACS for Windows NT Server version 3.0.1 is vulnerable and can be patched. Future versions of the software will include this patch. Please review the Workarounds section of this notice for detailed patch installation instructions.

The patch for this vulnerability can be downloaded from the following location if you are logged in with a valid CCO user account: <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-ac-win>

Workarounds

If you are unable to install the patch, user records that are "disabled" or "expired" in your NDS database should be temporarily removed until they are either valid again or the patch has been installed.

Install the patch according to the following directions:

1. Stop both "CSAUTH" and "CSAdmin" services by entering the following at the command prompt:

```
net stop CSAuth
net stop CSAdmin
```

2. Locate the <CSNTinstall>/Authenticators directory. For a default installation on the C:\ drive, the location will be the following: C:\Program Files\CiscoSecure ACS v3.0\Authenticators\NDSAAuth.dll.
3. Rename the original NDSAAuth.dll to something else (NDSAAuth_old.dll, for example) to save it.
4. Replace the original NDSAAuth.dll file with the patch file in its place.
5. Restart the services by entering the following at the command prompt:

```
net start CSAuth
net start CSAdmin
```

The patch is a single file and can be downloaded at the following location if you are logged in with a valid CCO user account: <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-ac-win>.

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

This vulnerability was discovered by internal Quality Assurance.

The Cisco PSIRT is not aware of any public announcements or 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 Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20020207-acs-nds-auth.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 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	2002–February–07	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: Feb 07, 2002

Document ID: 22198
