

Cisco Security Advisory: Multiple Vulnerabilities in CiscoSecure ACS for Windows NT Server

Document ID: 13624

Advisory ID: cisco-sa-20000921-secure-acs-nt

<http://www.cisco.com/warp/public/707/cisco-sa-20000921-secure-acs-nt.shtml>

Revision 1.3

Last Updated 2000 October 20 0800 UTC (GMT)

For Public Release 2000 September 21 1700 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

Multiple vulnerabilities have been identified and fixed in CiscoSecure ACS for Windows NT Server:

- The CSAdmin software module can be forced to crash by sending it an oversized URL. This defect is documented as Cisco bug ID **CSCdr68286**.
- CiscoSecure ACS for Windows NT Server can be placed into an unstable state by sending it an oversized TACACS+ packet. This defect is documented as Cisco bug ID **CSCdr51286**.
- The enable password can be bypassed to gain unauthorized privileges on a router or switch when CiscoSecure ACS for Windows NT Server is used in conjunction with an LDAP server that allows users to have null passwords. This defect is documented as Cisco bug ID **CSCdr26113**.

All releases of CiscoSecure ACS for Windows NT Server up to and including 2.1(x), 2.3(3), and 2.4(2) are vulnerable. These defects are fixed in release 2.4(3) and all subsequent releases. Free upgrades are offered to all affected customers as shown below. In lieu of an upgrade, several workarounds are available that might minimize the threat imposed by these defects.

CiscoSecure ACS for UNIX is not affected by these vulnerabilities.

Cisco Security Advisory: Multiple Vulnerabilities in CiscoSecure ACS for Windows NT Server

This advisory is available at
<http://www.cisco.com/warp/public/707/cisco-sa-20000921-secure-acs-nt.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The defects described in this document are present in releases 2.1(x), 2.3(3), and 2.4(2) of CiscoSecure ACS for Windows NT Server, as well as all earlier releases.

All three defects have been repaired in release 2.4(3). All subsequent releases of CiscoSecure ACS for Windows NT Server will include the fixes.

Products Confirmed Not Vulnerable

The previously mentioned releases of CiscoSecure ACS are vulnerable only if they are running on Windows NT Server. CiscoSecure ACS for UNIX is specifically not at risk due to these vulnerabilities.

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

Details

CSCdr68286

A buffer overflow condition within the CSAdmin module can be exploited by sending an oversized packet to TCP port 2002 of CiscoSecure ACS Server for Windows NT. Depending on the exact version of the underlying NT operating system, it may be possible to force the execution of inserted code or to temporarily crash the module. Any existing administrative sessions will be terminated when a crash occurs, which may lead to the loss of recent administrative actions. In versions 2.3(x) and higher, the CSAdmin module is restarted automatically within one minute. Existing sessions are re-established at that time, but the must be authenticated again as though they have started from the beginning. In earlier versions, the server must be restarted.

This vulnerability can be triggered without any authentication at all, although authentication is normally required for all expected activities.

CSCdr51286

By sending an oversized TACACS+ packet to CiscoSecure ACS for Windows NT Server it is possible to place the system into an unstable condition that may lead to a denial of service. In order to exploit this vulnerability, the attacker must be able to sniff or inject traffic into the path between the TACACS+ client and CiscoSecure ACS for Windows NT Server.

CSCdr26113

Some Lightweight Directory Access Protocol (LDAP) servers allow users to have a password that is undefined, meaning that the value of the stored password is null. An interaction between such an LDAP server and this defect may allow enable-mode authentication to succeed without specifying a valid password for that privileged mode.

Cisco Security Advisory: Multiple Vulnerabilities in CiscoSecure ACS for Windows NT Server

Impact

The following descriptions apply to all installations of CiscoSecure ACS for Windows NT Server. Installations of CiscoSecure ACS for UNIX are unaffected.

CSCdr68286

This defect can be exercised repeatedly to create a denial of service attack, thus affecting the availability of the server. Depending on specific Windows NT installation details, this defect can allow the unauthorized execution of arbitrary commands. This can be exploited to gain access to or modify data without appropriate authorization, thus possibly violating the confidentiality or integrity of the server.

CSCdr51286

This defect may be exercised repeatedly to create a denial of service attack, thus affecting the availability of the system.

CSCdr26113

If an LDAP server that allows null passwords is in use as described previously, then this defect can be exploited to escalate privileges on a network device without authorization.

Software Versions and Fixes

All versions of CiscoSecure ACS for Windows NT Server prior to release 2.4(3) are affected by all three vulnerabilities. Customers that are using any version earlier than release 2.4(3) should upgrade to 2.4(3) or higher.

Customers who are running any version of CiscoSecure ACS for UNIX are not vulnerable to the defects described in this security advisory.

Workarounds

The following workarounds will assist in mitigating threats due to these vulnerabilities, but cannot completely eliminate the potential for successful exploitation of the defects. Customers with affected systems are strongly recommended to upgrade to unaffected, fixed versions of the software as listed previously in this security advisory. In lieu of upgrading the software, the following steps may help minimize the risk:

CSCdr68286

To protect the CSAdmin module from oversized URLs, limit access to the CiscoSecure ACS server so that only computers with legitimate need can reach it via the network. This can be accomplished by placing an Access Control List (ACL) on a router between the CiscoSecure ACS server and the remainder of the network. In the following example, the CiscoSecure ACS server has an IP address of 1.1.1.1 and is attached to the Ethernet0 interface of an adjacent router. The terminal server has an address of 2.2.2.2. Access between the terminal server and the CiscoSecure ACS server can be prevented by entering config mode from enable mode and using commands similar to the following partial list of instructions to create an ACL and apply it to the router's Ethernet0 interface:

```
access-list 200 permit ip host 2.2.2.2 host 1.1.1.1 eq 49
access-list 200 deny any any log
```

```
interface Ethernet0
ip access-group 200 incoming
```

CSCdr51286

The CiscoSecure ACS server can be protected from receiving an oversized TACACS+ packet by applying an ACL on an adjacent router as shown above, or by implementing access controls on a firewall device that considers the ACS to be part of its protected network.

An additional method is to ensure that a trusted path exists between the CiscoSecure ACS for Windows NT Server and the devices that are using it. This is a prudent measure to prevent sniffing or injection of packets along that path.

CSCdr26113

Unauthorized enable access due to this defect can be thwarted by storing the enable password directly on the CiscoSecure ACS for Windows NT Server itself rather than on the remote LDAP 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

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities 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 advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20000921-secure-ac-s-nt.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
- firewalls@lists.gnac.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- 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 1.3	2000–October–20	Edited to ask customers to contact the TAC to obtain fixed software.
Revision 1.2	2000–September–21	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: Oct 20, 2000

Document ID: 13624
