

Cisco Security Advisory: Multiple Vulnerabilities in Cisco Secure Access Control Server

Document ID: 61603

Advisory ID: cisco-sa-20040825-acs

<http://www.cisco.com/warp/public/707/cisco-sa-20040825-acs.shtml>

Revision 1.3

Last Updated 2007 August 15 1600 UTC (GMT)

For Public Release 2004 August 25 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 for Windows (ACS Windows) and Cisco Secure Access Control Server Solution Engine (ACS Solution Engine) provide authentication, authorization, and accounting (AAA) services to network devices such as a network access server, Cisco PIX and a router. This advisory documents multiple Denial of Service (DoS) and authentication related vulnerabilities for the ACS Windows and the ACS Solution Engine servers.

The vulnerabilities are documented as these Cisco bug IDs:

- [CSCeb60017](#) ([registered](#) customers only)
- [CSCec66913](#) ([registered](#) customers only)
- [CSCec90317](#) ([registered](#) customers only)
- [CSCed81716](#) ([registered](#) customers only)
- [CSCef05950](#) ([registered](#) customers only)

This advisory will be posted at <http://www.cisco.com/warp/public/707/cisco-sa-20040825-acs.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

These products are vulnerable:

- Versions 3.2(3) and earlier are vulnerable to [CSCef05950](#) ([registered](#) customers only) and [CSCed81716](#) ([registered](#) customers only) .
- Version 3.2(2) build 15 is vulnerable to [CSCeb60017](#) ([registered](#) customers only) .
- Version 3.2 is vulnerable to [CSCec90317](#) ([registered](#) customers only) and [CSCec66913](#) ([registered](#) customers only) .

[CSCed81716](#) is only applicable to the ACS Solution Engine.

Successfully authenticate to your ACS box to determine your software revision. After you perform the authentication, the first screen displays the current ACS version in this format CiscoSecure ACS Release 3.2(3) Build 11.

ACS versions may also be displayed as 003.002(003.011), where "011" is the build number referenced on the ACS graphical user interface (GUI).

Products Confirmed Not Vulnerable

Cisco Secure ACS for UNIX is not affected by these vulnerabilities. No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The Cisco Secure ACS products provide a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. The products help to ensure enforcement of assigned policies they allow network administrators to control who can log into the network, per user privileges in the network, security auditing and billing information, and command level access controls.

- [CSCeb60017](#) ([registered](#) customers only) and [CSCec66913](#) ([registered](#) customers only) — Cisco Secure ACS provides a Web-based management interface, termed CSAdmin, which listens on TCP port 2002. When flooded with TCP connections the ACS Windows and ACS Solution Engine stops responding to any new TCP connections destined for port 2002. Additionally, services on the ACS that process authentication related requests may become unstable and stop responding, which hampers the ability for ACS to process any authentication related requests. A reboot of the device is required to restore these services.
- [CSCec90317](#) ([registered](#) customers only) — Cisco Secure ACS, when configured for Light Extensible Authentication Protocol (LEAP) RADIUS Proxy, forwards LEAP authentication requests to a secondary RADIUS server. The ACS device with LEAP RADIUS proxy configured may crash when LEAP authentication requests are being processed. A reboot is required to bring the device back to an operational state.
- [CSCed81716](#) ([registered](#) customers only) — Cisco Secure ACS can communicate with external databases and authenticate users against those databases. One of the external databases that ACS supports is Novell Directory Services (NDS). If an anonymous bind in NDS is allowed, and if the ACS Solution Engine is authenticating NDS users with NDS as the external database and not Generic

LDAP, then users are able to authenticate with blank passwords against that NDS database. However, wrong passwords and incorrect usernames are properly rejected.

- [CSCef05950](#) ([registered customers only](#)) — Once a user successfully authenticates to the ACS GUI on TCP port 2002, a separate TCP connection is created between the browser and ACS administration Web service, with a random destination port. If an attacker spoofs the IP address of the user computer, and accesses the ACS GUI on this random port, then the attacker may be able to connect to the ACS GUI, bypassing authentication. Authentication to the ACS server may also be bypassed if the attacker is behind the same PAT device as that of the ACS user and accesses the ACS GUI on this random port.

Impact

This section describes the impact of these vulnerabilities.

- [CSCeb60017](#) ([registered customers only](#)) , [CSCec66913](#) ([registered customers only](#)) , and [CSCec90317](#) ([registered customers only](#)) — Exploitation of these vulnerabilities may cause a shutdown of core services, impacting the availability of services on the ACS devices, which will persist until the device is rebooted. This results in a Denial of Service for the ACS device, which can potentially cause authentication to be bypassed, depending on the configuration of AAA clients within the network.
- [CSCed81716](#) ([registered customers only](#)) — This vulnerability may allow unauthorized users to access AAA clients without an effective password (using blank passwords) if the bind to the NDS database is anonymous.
- [CSCef05950](#) ([registered customers only](#)) — This vulnerability may allow unauthenticated users to gain access to the ACS Administration GUI.

Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

DDTs Bug ID	Impacted Versions	Fixed Versions	Platform
CSCeb60017 (registered customers only)	3.2(1), 3.2(2)	003.002(002.020) or later, 3.2(3) in Product Upgrade Tool	ACS Windows and ACS Solution Engine
CSCec66913 (registered customers only)	3.2(1), 3.2(2)	003.002(002.020) or later, 3.2(3) in Product Upgrade Tool	ACS Windows and ACS Solution Engine
CSCec90317 (registered customers only)	3.2(1)	003.002(002.005) or later, 3.2(2) in Product Upgrade Tool	ACS Windows and ACS Solution

			Engine
CSCed81716 (registered customers only)	3.2(1), 3.2(2)	003.002(003.011) or later, 3.2(3) in Product Upgrade Tool	ACS Solution Engine only
CSCef05950 (registered customers only)	3.0(x), 3.1(x), 3.2(x), 3.3(1)	<p>There are patches available to address this vulnerability for versions 3.1(2), 3.2(3) and 3.3(1). See the Customers with Service Contracts section below for details on the location of these patches.</p> <p>Although version 3.0 is affected, the fix is only available with a feature set included in versions 3.1 and higher. Customers without Service Contracts will need to contact Cisco Technical Assistance Center at the numbers listed below for assistance.</p>	ACS Windows and ACS Solution Engine

Upgrade procedures can be found as indicated:

- ACS Windows 3.3:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/installation
- ACS Windows 3.2:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guide09186a0080184928.html#w
- ACS Solution Engine:
http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_user_guide_chapter09186a0080204d45.html#w

Workarounds

This section describes workarounds for these vulnerabilities.

- Configure an IP address filter on ACS Windows and ACS Solution Engine to limit the exposure of these vulnerabilities. From within the ACS GUI, browse to **Administration Control > Access Policy** to limit access to only the machines that need to administer the ACS remotely.
- Apply access control lists (ACLs) on routers, switches and firewalls that filter traffic to the ACS so that traffic is only allowed from stations that need to remotely administer the box. Refer to <http://www.cisco.com/warp/public/707/tacl.html> for examples on how to apply ACLs on Cisco routers.
- As a best practice, use HTTPS to limit access to the Cisco ACS GUI. Issues detailed in [CSCef05950](#) ([registered](#) customers only) still exist when you use HTTP instead of HTTPS to access the Cisco ACS GUI.

Refer to

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs32/user02/a.htm#wp89030 for information on how to set up an access policy on the Cisco ACS.

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 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 advisory will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040825-ac.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
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com

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	2007-August-14	Fixed link.
Revision 1.2	2004-October-05	Clarified impact of Denial of Service vulnerabilities in the Impact section. Added the Impacted Versions column and added content to the Fixed Versions column in the Software Versions and Fixes section table. Clarified version 3.0(x) status in the Software Versions and Fixes section.

Revision 1.1	2004–August–25	Changed URLs in the Obtaining Fixed Software section.
Revision 1.0	2004–August–25	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: Aug 14, 2007

Document ID: 61603
