

Table of Contents

Cisco Security Advisory: Cisco Security Advisory: Cisco Secure Access Control Server for Windows Admin Buffer Overflow Vulnerability.....1

Document ID: 42301.....1

Revision 1.2.....1

Last Updated 2003 May 07 14:20 (GMT).....1

For Public Release 2003 April 23 08:00 (GMT).....1

Please provide your feedback on this document.....1

Summary.....1

Affected Products.....1

Details.....2

Impact.....2

Software Versions and Fixes.....2

Obtain Fixed Software.....2

Workarounds.....3

Exploitation and Public Announcements.....3

Status of This Notice: Final.....4

Distribution.....4

Revision History.....4

Cisco Security Procedures.....4

Cisco Security Advisory: Cisco Security Advisory: Cisco Secure Access Control Server for Windows Admin Buffer Overflow Vulnerability

Document ID: 42301

Revision 1.2

Last Updated 2003 May 07 14:20 (GMT)

For Public Release 2003 April 23 08:00 (GMT)

Please provide your feedback on this document.

- Summary
- Affected Products
- Details
- Impact
- Software Versions and Fixes
- Obtain Fixed Software
- Workarounds
- Exploitation and Public Announcements
- Status of This Notice: Final
- Distribution
- Revision History
- Cisco Security Procedures

Summary

Cisco Secure Access Control Server (ACS) for Windows is vulnerable to a buffer overflow on the administration service which runs on TCP port 2002. The exploitation of this vulnerability results in a Denial of Service, and can potentially result in system administrator access. Cisco provides repaired software, and Cisco advises customers to install patches or upgrade at their earliest opportunity. Workarounds can be implemented, that include how to block external access to port 2002 on the ACS.

This issue is documented in Cisco Bug ID CSCea51366. This issue is also referenced in the Mitre CVE as CAN-2003-0210.

Affected Products

Cisco Secure ACS versions up to and including version 2.6.4 , 3.0.3, and 3.1.1 are affected by this vulnerability.

No other Cisco products are affected by this vulnerability. Specifically, Cisco Secure ACS for UNIX is NOT affected.

Details

Cisco Secure ACS for Windows provides a Web-based management interface, termed Cisco Secure Admin, which listens on TCP port 2002. A buffer overflow vulnerability occurs during Cisco Secure Admin process servicing login requests. A sufficiently long user parameter is received by the server can cause the buffer overflow, which typically results in a service hang until it is restarted. It is possible that a buffer overflow be performed that results in the compromise of the system and permit remote control of the system.

This issue is resolved when you apply the patch files to repair the Cisco Secure Admin program, and will be repaired in future versions of Cisco Secure Admin.

- Bug ID CSCea51366

Impact

Customer installations of Cisco Secure ACS for Windows that provide unrestricted access to all ports on the server can potentially be vulnerable to a Denial of Service, or potentially a root compromise. Cisco advises customers to upgrade to repaired versions of Cisco Secure ACS, or install Cisco Secure ACS such that external access to management interfaces is eliminated or severely restricted.

Software Versions and Fixes

Fixes to the Cisco Secure Admin will be included in ACS for Windows versions 3.0.4, 3.1.2, and later, which will become available on the Cisco website. The patch files for 2.6.4, 3.0.3, and 3.1.1 are currently available on the Cisco website. Customers who run versions earlier than 2.6.4, 3.0.3, or 3.1.1 need to upgrade to those versions to apply the patch files.

The patch files that resolve this problem for specific versions are:

- ACS 3.1(1) Cisco Secure Admin-Patch-3.1-1-27.zip (Follow the link included in this document regarding strong encryption known as 3DES to download this patch.)
- ACS 3.0(3) Cisco Secure Admin-Patch-3.0-3-6.zip
- ACS 2.6 Cisco Secure Admin-patch-2.6-4-4.zip

Customers can download these files here: <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-acs-win>.

Customers that need the patch for ACS 3.1(1), should select the link titled "Download Access Control Server for Windows Patches (Strong Cryptographic 3DES Software)".

When you consider software upgrades, also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers must exercise caution to make sure the devices to be upgraded contain sufficient memory and that current hardware and software configurations continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) for assistance.

Obtain Fixed Software

Cisco offers free software upgrades to remedy this vulnerability for all affected customers. Customers can

Cisco Security Advisory: Cisco Security Advisory: Cisco Secure Access Control Server for Windows Admin

only install and expect support for the feature sets they have purchased.

Customers with contracts must obtain upgraded software through their regular update channels. For most customers, this means that upgrades must be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers whose Cisco products are provided or maintained through prior agreement or an agreement that is in existence now with third-party support organizations such as Cisco Partners, authorized resellers, or service providers must contact that support organization for assistance with the upgrade, which should be free of charge.

Customers who purchase directly from Cisco but who do not hold a Cisco service contract and customers who purchase through the third-party vendors but are not able to obtain fixed software through their point of sale, must get their upgrades or patch files through the Cisco Technical Assistance Center (TAC). In those cases, customers can only upgrade to a later version of the same release to which they are entitled, or the patch files for that release. TAC contacts are:

- +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

For additional TAC contact information, which includes special localized telephone numbers and instructions and e-mail addresses for use in various languages, refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

You must 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.

Do not contact either psirt@cisco.com or security-alert@cisco.com for software upgrades.

Customers can only install and expect support for the feature sets they have purchased. When you install download, access or otherwise use such software upgrades, you must 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>.

Workarounds

Cisco advises you to patch the system, or upgrade to repaired versions of Cisco Secure ACS. Alternatively, the vulnerability can be mitigated when access to the ACS is blocked on the port 2002, as well as if you strictly limit the access to internal hosts that have reason to connect to the ACS. This can be accomplished with access control lists on routers or firewalls.

Exploitation and Public Announcements

The Cisco PSIRT was made aware of this vulnerability by the NSFOCUS Security Team, who are also releasing an advisory with regard to this issue. Their advisory will be available at <http://www.nsfocus.com/english/homepage/research/0304.htm>.

Cisco is unaware of malicious use of the vulnerabilities described in this advisory.

Status of This Notice: Final

This is a final notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all the facts have been checked to the best of their ability. Cisco does not anticipate to issue updated versions of this notice unless there is some material change in the facts. Should there be a significant change in the facts, Cisco can update this notice.

Distribution

This notice is posted on the Cisco worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20030423-ACS.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 these e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@securityfocus.com
- full-disclosure@lists.netsys.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on the Cisco worldwide web. Users concerned about this problem are encouraged to check the URL given in this document for any updates.

Revision History

Revision 1.0	2003-April-23	Initial public release
Revision 1.1	2003-April-23	Clarified location of 3.1(1) patch files in "Software Versions and Fixes" section
Revision 1.2	2003-May-07	Additional clarification to 3.1.1 patch location

Cisco Security Procedures

Complete information on how to report security vulnerabilities in Cisco products, to obtain assistance with security incidents, and on how to register to receive security information from Cisco, is available on the Cisco worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries with regard to Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.
