

Cisco Security Advisory: Cisco Security Agent Management Center LDAP Administrator Authentication Bypass

Document ID: 71954

Advisory ID: cisco-sa-20061101-csamc

<http://www.cisco.com/warp/public/707/cisco-sa-20061101-csamc.shtml>

Revision 1.0

For Public Release 2006 November 01 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Version and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Cisco Security Agent Management Center (CSAMC) contains an administrator authentication bypass vulnerability when configured to use an external Lightweight Directory Access Protocol (LDAP) server for authentication.

There is a workaround for this vulnerability. Cisco has made free software available to address this vulnerability for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20061101-csamc.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

CSAMC version 5.1 prior to Hotfix 5.1.0.79 is affected by this vulnerability.

Products Confirmed Not Vulnerable

CSAMC versions prior to 5.1 are not affected by this vulnerability. No other Cisco products are currently known to be affected by this vulnerability.

Details

Cisco Security Agent Management Center (CSAMC) version 5.1 contains an administrator authentication bypass vulnerability when configured to authenticate administrators against an external LDAP server.

There are three roles for CSAMC administrators: configure, deploy, and monitor. The configure role has complete access to the CSAMC application, including the ability to create security policies. The deploy role can create agent kits, deploy security policies, and perform application monitoring. The deploy role cannot modify security policies. The monitoring role can only perform application monitoring functions.

All CSAMC administrator accounts are defined in the local CSAMC database and have an assigned role. CSAMC can be configured to use an external LDAP server to authenticate administrators. As a safety feature, it is possible to specify certain administrator accounts to fall back to local authentication if the LDAP server is unavailable.

If CSAMC is configured to use LDAP for authentication, it is possible to supply a valid administrator username and blank (zero length) password and gain administrative access to the CSAMC application with the role privileges of the administrator. This vulnerability occurs when CSAMC incorrectly handles an authentication failure message from the LDAP server. The administrator password stored on the LDAP server is a valid, non-blank password.

CSAMC version 5.1 is the first to include external LDAP authentication. LDAP authentication is not the default configuration for CSAMC and must be explicitly configured. The LDAP server in this configuration is not built into CSAMC.

Information on configuring administrator LDAP authentication for CSAMC can be found here:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008066e98e.html

Information on configuring role-based administration for CSAMC can be found here:

http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_configuration_guide_chapter09186a008066e98e.html

This vulnerability is documented in Cisco Bug ID [CSCsg40822](#) ([registered](#) customers only) .

Impact

Successful exploitation of this vulnerability allows an attacker with a valid administrator username to gain access to the CSAMC application with the role privileges of the compromised administrator account. If the administrator has a role of configure or deploy, it is possible to make policy changes for managed CSA clients. This may be leveraged to reduce the security posture of managed systems and allow potential attacks against the managed systems.

Software Version 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.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:

<http://www.cisco.com/warp/public/620/1.html>

Fixed CSAMC (fcs-csamc-hotfix-5.1.0.79-w2k-k9.zip) software can be downloaded at <http://www.cisco.com/cgi-bin/tablebuild.pl/csa-h-crypto?psrtdcat20e2>.

Affected Software Version	Fixed Software Version
CSAMC version 5.1 Hotfix prior to 5.1.0.79	CSAMC version 5.1 Hotfix 5.1.0.79

Workarounds

It is possible to workaround this vulnerability by disabling external LDAP authentication and configuring administrators to authenticate against the local CSAMC database.

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.

This vulnerability was reported to Cisco by a third party.

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 is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20061101-csamc.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
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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 1.0	2006-November-01	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>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 01, 2006

Document ID: 71954
