

Cisco Security Advisory: Cisco ACE Application Control Engine Device Manager and Application Networking Manager Vulnerabilities

Advisory ID: cisco-sa-20090225-anm

<http://www.cisco.com/warp/public/707/cisco-sa-20090225-anm.shtml>

Revision 1.0

For Public Release 2009 February 25 1600 UTC (GMT)

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

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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 exist in the Cisco Application Networking Manager (ANM) and Cisco Application Control Engine (ACE) Device Manager applications. These vulnerabilities are independent of each other. Successful exploitation of these vulnerabilities may result in unauthorized system or host operating system access.

This security advisory identifies the following vulnerabilities:

- ACE Device Manager and ANM invalid directory permissions vulnerability
- ANM default user credentials vulnerability
- ANM MySQL default credentials vulnerability
- ANM Java agent privilege escalation

Cisco has released free software updates that address these vulnerabilities. A workaround that mitigates one of the issues is available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090225-anm.shtml>.

Note: This advisory is being released simultaneously with a multiple vulnerabilities advisory impacting the ACE appliance and module software, which is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20090225-ace.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

The following are the products and versions affected by each vulnerability described within this advisory.

Vulnerability	Product Affected	Version Affected
---------------	------------------	------------------

Invalid Directory Permissions	ACE Device Manager	All versions prior to A3 (2.1)
Invalid Directory Permissions	ANM	All versions prior to ANM 2.0
Default User Credentials	ANM	All versions prior to ANM 2.0
MySQL Default Credentials	ANM	All versions prior to ANM 2.0
Java Agent Privilege Escalation	ANM	All versions prior to ANM 2.0 Update A

Determining ACE Device Manager Software Version

The ACE Device Manager is embedded with the ACE appliance software.

To display the version of system software that is currently running on the device, use the **show version** command. The following example includes the output of the show version command on a Cisco ACE appliance running software version A3(2.1):

```
ACE-4710/Admin# show version
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 1985-2008 by Cisco Systems, Inc. All
rights reserved.
The copyrights to certain works contained herein are
owned by
other third parties and are used and distributed under
license.
Some parts of this software are covered under the GNU
Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
```

```
Software
  loader:      Version 0.95
```

```
system:      Version A3(2.1) [build 3.0(0)A3(2.1)
adbuild_14:33:29-2008/11/19_/auto/adbu-rel4/
rel_a3_2_1_throttle_build/REL_3_0_0_A3_2_1]
system image file: (nd)/192.168.65.32/scimitar.bin
Device Manager version 1.1 (0) 20081113:2052
---
```

Determining ANM Software Version

To display the version of ANM software that is currently installed, login to the ANM server and select the **About** keyword in the upper right. An informational pop up window will be displayed. ANM Version 2.0 Update A is indicated in the example output below.

```
Version: 2.0(0), Update: A
Build Number: 709
Build Timestamp: 20081031:1226
```

☐ Products Confirmed Not Vulnerable

The Cisco ACE XML Gateway, Cisco ACE GSS (Global Site Selector) 4400 Series and Cisco ACE Web Application Firewall are not affected by any of these vulnerabilities.

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

[Top of the section](#) [Close Section](#)

☐ Details

ANM is a network management application that manages Cisco ACE modules or appliances. ANM is installed on customer provided servers with a Red Hat Enterprise Linux operating system. The ACE Device Manager provides a browser-based interface for configuring and managing a single ACE appliance. The ACE Device Manager resides in flash memory on the ACE appliance. Multiple vulnerabilities exist in ANM and one in the ACE Device Manager products. The following details are provided for each vulnerability addressed in this security advisory.

Invalid Directory Permissions

Versions of the Cisco ACE Device Manager prior to software version A3(2.1) and Cisco ANM prior software version ANM 2.0 contain directory traversal vulnerabilities. These vulnerabilities could allow unauthorized access to ACE operating system and host operating system files. To exploit

these vulnerabilities authentication is required to initially access either product.

This vulnerability is documented in the following Cisco Bug IDs:

- [CSCsv66063](#) ([registered](#) customers only)
- [CSCsv70130](#) ([registered](#) customers only)

This vulnerability has been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0615.

Default User Credentials

Versions of Cisco ANM prior to software version ANM 2.0 do not force credential changes during installation. If these credentials are left unchanged, this could allow unauthorized access to the ANM application with default user credentials.

This vulnerability is documented in the following Cisco Bug ID:

- [CSCsu52724](#) ([registered](#) customers only)

This vulnerability has been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0616.

MySQL Default Credentials

ANM versions prior to ANM 2.0 use a default MySQL root user password during installation. The MySQL database is installed by default when ANM is initially installed. This vulnerability can be exploited remotely with default credential authentication and without end-user interaction. Unauthorized access to the database may allow modification of system files that could impact the function of ANM or allow execution of commands on the underlying host operating system. The ACE appliance and module device configuration files in the MySQL database are encrypted.

This vulnerability is documented in the following Cisco Bug ID:

- [CSCsu52632](#) ([registered](#) customers only)

This vulnerability has been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0617.

Java Agent Privilege Escalation

ANM versions prior to ANM 2.0 Update A contain a remotely exploitable vulnerability that could allow an attacker to view configuration files and modify ANM processes including the capability to stop services. Exploitation of this issue could result in system information disclosure or denial of services.

This vulnerability is documented in the following Cisco Bug ID:

- [CSCsu73001](#) ([registered](#) customers only)

This vulnerability has been assigned the Common Vulnerability and Exposures (CVE) ID CVE-2009-0618.

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsv66063 - ACE Device Manager invalid directory permissions

Calculate the environmental score of [CSCsv66063](#)

CVSS Base Score - 9					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - 7.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsv70130 - ANM invalid directory permissions

Calculate the environmental score of [CSCsv70130](#)

CVSS Base Score - 9					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - 7.4					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsu52724 - ANM default user credentials during installation

Calculate the environmental score of [CSCsu52724](#)

CVSS Base Score - 10					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - 8.7					
Exploitability		Remediation Level		Report Confidence	
High		Official-Fix		Confirmed	

CSCsu52632 - ANM embedded MySQL default credentials

Calculate the environmental score of [CSCsu52632](#)

CVSS Base Score - **10**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Complete	Complete	Complete

CVSS Temporal Score - **8.7**

Exploitability	Remediation Level	Report Confidence
High	Official-Fix	Confirmed

CSCsu73001 - ANM Java agent privilege escalation

Calculate the environmental score of [CSCsu73001](#)

CVSS Base Score - **8.5**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	Partial	None	Complete

CVSS Temporal Score - **7.4**

Exploitability	Remediation Level	Report Confidence
High	Official-Fix	Confirmed

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of the ACE Device Manager and ANM invalid directory permission vulnerabilities may allow unauthorized access to view or modify the ACE Device Manager or ANM file system, including host operating system files. Modification of some system files could result in a denial of service condition.

Exploitation of the ANM default user credential and ANM MySQL database default credential vulnerabilities may allow an attacker to gain unauthorized system access. Modification of ANM settings with the default user credentials could result in a denial of service condition. Unauthorized access to the MySQL database may allow modification of system files that could impact the function of ANM or allow execution of commands on the underlying host operating system.

Successful exploitation of the ANM privilege escalation vulnerability may result in unauthorized remote access to system processes and services with the ability to modify. Modification of these services could result in a denial of service condition.

[Top of the section](#) [Close Section](#)

☐ 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.

Each row of the following software table identifies the earliest possible software release that contains the fix listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the release which have fixes for all the published vulnerabilities at the time of this Advisory.

Vulnerability	First Fixed Release	Recommended Release
ACE Device Manager Invalid Directory Permissions	A3(2.1)	A3(2.1)
ANM Invalid Directory Permissions	ANM 2.0	ANM 2.0 Update A

ANM Default User Credentials	ANM 2.0	ANM 2.0 Update A
ANM MySQL Default Credentials	ANM 2.0	ANM 2.0 Update A
ANM Java Agent Privilege Escalation	ANM 2.0 Update A	ANM 2.0 Update A

ANM 2.0 Update A can be downloaded from [ANM 2.0 UPDATE A](#).

ACE Device Manager A3(2.1) can be downloaded from [ACE A3\(2.1\)](#).

[Top of the section](#) [Close Section](#)

☐ Workarounds

While this Security Advisory describes multiple distinct vulnerabilities, a workaround exists for only the following vulnerability.

ANM Default User Credentials

The ANM user *admin* account password may be modified after installation by following the procedures documented for [Changing the Admin Password](#) located in the ANM User Guide.

Applied Mitigation Bulletin

Additional mitigation techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20090225-anm.shtml>

[Top of the section](#) [Close Section](#)

☐ Obtaining Fixed Software

Cisco has released free software updates that address these vulnerabilities. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract

customers must be requested through the TAC.

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

Acknowledgement to the National Australia Bank's Security Assurance team for the discovery and reporting of the ACE Device Manager directory permissions vulnerability.

The remaining vulnerabilities were identified through internal testing.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090225-anm.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-bulletins@lists.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.

[Top of the section](#) [Close Section](#)

☐ Revision History

Revision 1.0	2009-February-25	Initial public release
--------------	------------------	------------------------

[Top of the section](#) [Close Section](#)

☐ 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>.

[Top of the section](#) [Close Section](#)

Help us help you.



Please rate this document.



Excellent

Good

Average

Fair

Poor



This document solved my problem.



Yes

No

Just browsing



Suggestions for improvement:

(256 character limit)



[Home](#)

[How to Buy](#)

[Login](#)

[Profile](#)

[Feedback](#)

[Site Map](#)

[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)