

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco ANM

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-079>

Gestion du document

Référence	CERTA-2009-AVI-079
Titre	Vulnérabilités dans Cisco ANM
Date de la première version	26 février 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20090225-anm du 25 février 2009
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Accès à distance au système ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- *Cisco ACE Device Manager* versions antérieures à A3(2.1) ;
- *Cisco ANM* versions antérieures à 2.0.

3 Résumé

Plusieurs vulnérabilités dans *Cisco ANM* permettent d'accéder au système à distance et de procéder à une élévation de privilèges.

4 Description

Plusieurs vulnérabilités ont été découvertes dans *Cisco ANM (Application Networking Manager)* :

- des traversées de répertoires sont possibles, ce qui permet à un utilisateur authentifié d’avoir accès à des fichiers système (CVE-2009-0615) ;
- le compte `Default User` possède un mot de passe par défaut dont le remplacement n’est pas rendu obligatoire lors de l’installation. Il est par conséquent possible d’obtenir un accès à distance sur ce compte (CVE-2009-0616) ;
- le compte administrateur de la base `MySQL` possède un mot de passe par défaut (CVE-2009-0617) ;
- l’agent `Java` contient une vulnérabilité qui permet un accès en lecture à distance à des fichiers de configuration, ainsi que la modification de certains processus en cours (avec notamment la possibilité d’arrêter certains services) (CVE-2009-0618).

5 Solution

Se référer au bulletin de sécurité de l’éditeur pour l’obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco 20090225-anm du 25 février 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20090225-anm.shtml>
- Référence CVE CVE-2009-0615 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0615>
- Référence CVE CVE-2009-0616 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0616>
- Référence CVE CVE-2009-0617 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0617>
- Référence CVE CVE-2009-0618 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0618>

Gestion détaillée du document

26 février 2009 version initiale.