Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 26 février 2009
N° CERTA-2009-AVI-078

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco ACE

Gestion du document

Référence	CERTA-2009-AVI-078
Titre	Multiples vulnérabilités dans Cisco ACE
Date de la première version	26 février 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20090225-ace 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 au système avec des droits administrateur ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- *Cisco ACE 4710* versions antérieures à A3(2.1) ou à A1(8a) ;
- *Cisco ACE Module* versions antérieures à A2(1.3).

3 Résumé

De multiples vulnérabilités dans *Cisco ACE* permettent, entre autres, d'accéder au système avec des droits d'administration.

4 Description

De multiples vulnérabilités ont été découvertes dans *Cisco ACE* (*Application Control Engine*) :

- des noms d'utilisateur avec mot de passe par défaut permettent des accès distants à divers comptes d'administration (CVE-2009-0620 et CVE-2009-0621) ;
- une élévation des privilèges est possible via l'interface en ligne de commande `CLI` (CVE-2009-0622) ;
- un déni de service à distance est possible par l'envoi d'un paquet `SSH` spécifiquement constitué (CVE-2009-0623) ;
- un utilisateur authentifié peut provoquer un déni de service à l'aide d'un paquet `SNMPv2` spécifiquement constitué (CVE-2009-0624) ;
- l'envoi d'un paquet `SNMPv3` spécifique peut provoquer un déni de service à distance (CVE-2009-0625).

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-ace du 25 février 2009 :
  http://www.cisco.com/warp/public/707/cisco-sa-20090225-ace.shtml
- Référence CVE CVE-2009-0620 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0620
- Référence CVE CVE-2009-0621 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0621
- Référence CVE CVE-2009-0622 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0622
- Référence CVE CVE-2009-0623 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0623
- Référence CVE CVE-2009-0624 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0624
- Référence CVE CVE-2009-0625 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0625

Gestion détaillée du document

26 février 2009 version initiale.