

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'authentification sur Cisco Secure Access Control Server

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-2002-AVI-026>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2002-AVI-026 |
| Titre | Vulnérabilité dans l'authentification sur Cisco Secure Access Control Server |
| Date de la première version | 08 février 2002 |
| Date de la dernière version | – |
| Source(s) | Avis Cisco |
| 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

Contournement des règles de sécurité.

2 Systèmes affectés

Cisco Secure Access Control Server (ACS) version 3.0.1 configuré pour utiliser le serveur Novell Directory Service (NDS).

3 Résumé

Des utilisateurs non autorisés peuvent s'authentifier, quelque soit leur statut dans le serveur NDS.

4 Description

Cisco Secure Access Control Server est un outil qui permet de centraliser le contrôle des accès des utilisateurs aux passerelles du réseau. Il peut être configuré pour faire appel au service NDS.

Une vulnérabilité de Cisco Secure ACS permet à des utilisateurs dont les comptes sont désactivés ou ont expiré dans NDS de s'authentifier normalement.

5 Solution

Appliquer le correctif Cisco :
<http://www.cisco.com/cgi-bin/tablebuild.pl/cs-acis-win>

6 Documentation

Avis Cisco :
<http://www.cisco.com/warp/public/707/ciscosecure-acis-nds-authentication-vuln-pub.shtml>

Gestion détaillée du document

08 février 2002 version initiale.