



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 janvier 2006
N° CERTA-2006-AVI-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur CISCO ACS

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-2006-AVI-004>

Gestion du document

Référence	CERTA-2006-AVI-004
Titre	Vulnérabilité sur CISCO ACS
Date de la première version	04 janvier 2006
Date de la dernière version	–
Source(s)	Information CISCO du 26 décembre
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 de la politique de sécurité.

2 Systèmes affectés

- VPN3000 Concentrator ;
- VPN3000 Hardware Client 3.x ;
- Cisco versions Pix 6.x antérieures à la version 6.3(5) ;
- Cisco versions Pix 7.x antérieures à la version 7.0(2) ;
- Cisco Firewall Services Module (FWSM) 1.x ;
- Cisco Firewall Services Module (FWSM) 2.x ;
- Cisco Secure versions ACS 3.x antérieures à la version 4.0.1.

3 Résumé

Une vulnérabilité présente dans Cisco Secure ACS (Access Control Server) peut être exploitée par un utilisateur mal intentionné du réseau local pour contourner la politique de sécurité mise en place.

4 Description

La vulnérabilité présente sur Cisco Secure ACS est due à une erreur de conception dans le téléchargement des IP ACL.

Un utilisateur mal intentionné peut, en utilisant le nom du fichier de téléchargement des IP ACL, s'authentifier au serveur d'authentification (RAS/NAS) et ainsi contourner la politique de sécurité.

5 Solution

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

6 Documentation

– Information Cisco du 26 décembre 2006 :

http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_fiel_notice09186a00805bf1c4.shtml

Gestion détaillée du document

04 janvier 2006 version initiale.