



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 janvier 2007
N° CERTA-2007-AVI-012

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Cisco secure 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-2007-AVI-012>

Gestion du document

Référence	CERTA-2007-AVI-012
Titre	Multiples vulnérabilités de Cisco secure ACS
Date de la première version	08 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin Cisco ID 77820
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

Cisco Secure Access Control Server version 4.0 et précédentes.

3 Résumé

Cisco Secure Access Control Server sert à l'authentification et au contrôle d'accès. Plusieurs vulnérabilités permettent à un utilisateur malveillant de provoquer un déni de service à distance et/ou une exécution de code arbitraire.

4 Description

Plusieurs vulnérabilités permettent à un utilisateur malveillant de provoquer un déni de service à distance et/ou une exécution de code arbitraire :

- Une vulnérabilité dans le traitement des requêtes HTTP GET provoque un débordement de pile et un arrêt du service CSAdmin. Elle peut être exploitée pour l'exécution de code arbitraire.
- Une vulnérabilité dans le traitement des requêtes RADIUS Accounting-Request provoque un débordement de pile et un arrêt du service CSRADIUS. Elle peut être exploitée pour l'exécution de code arbitraire.
- Une vulnérabilité dans le traitement des requêtes RADIUS Access-Request provoque un arrêt du service CSRADIUS.

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 ID 77820 du 05 janvier 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070105-csacs.shtml>

Gestion détaillée du document

08 janvier 2007 version initiale.