

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco Secure ACS pour Windows

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-070>

Gestion du document

Référence	CERTA-2002-AVI-070
Titre	Vulnérabilités dans Cisco Secure ACS pour Windows
Date de la première version	05 avril 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco "Web Interface Vulnerabilities in Cisco ACS for Windows"
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

- Déni de service ;
- exécution de code arbitraire ;
- accès à des données non autorisées.

2 Systèmes affectés

- Cisco Secure ACS pour Windows version 2.6.x ;
- Cisco Secure ACS pour Windows version 3.0.1 (build 40).

3 Résumé

Deux vulnérabilités ont été trouvées dans Cisco Secure ACS pour Windows.

4 Description

Cisco Secure Access Control Server (ACS) est un outil de centralisation des autorisations d'accès (AAA). ACS possède un module d'administration distante CSADMIN utilisant le port TCP 2002. Deux vulnérabilités sont présentes dans ce module :

- L'envoi d'une URL particulière peut permettre de stopper le module et, dans certains cas, d'exécuter du code arbitraire.
- Un utilisateur mal intentionné peut également accéder à certaines données du disque ou de la partition où se situe l'installation du module en employant une syntaxe spécifique dans l'URL afin de remonter en dehors de la racine du serveur Web.

5 Contournement provisoire

Filtrer le port 2002/TCP sur un équipement de filtrage en amont afin d'empêcher les accès non autorisés.

6 Solution

Se référer au bulletin de sécurité Cisco pour consulter les correctifs disponibles (cf. Documentation).

7 Documentation

Bulletin de sécurité Cisco "Web Interface Vulnerabilities in Cisco Secure ACS" disponible à l'adresse suivante :

<http://www.cisco.com/warp/public/707/ACS-Win-Web.shtml>

Gestion détaillée du document

05 avril 2002 version initiale.