

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2004-AVI-279>

Gestion du document

Référence	CERTA-2004-AVI-279
Titre	Multiples vulnérabilités dans Cisco Secure ACS
Date de la première version	26 août 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

- Déni de service ;
- Atteinte à la confidentialité des données.

2 Systèmes affectés

- Cisco Secure ACS versions 3.2(3) et antérieures pour Windows ;
- Cisco Secure ACS version 3.2(2) build 15 pour Windows ;
- Cisco Secure ACS version 3.2 pour Windows ;
- Cisco Secure ACS solution Engine.

3 Résumé

Plusieurs vulnérabilités présentes dans Cisco Secure ACS (Access Control Server) pour Windows permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'accéder à des données confidentielles.

4 Description

Cisco Secure ACS et Cisco Secure ACS Solution Engine sont des logiciels qui fournissent le service AAA (Authentication, Authorization, Accounting) vers les équipements réseau tels que les serveurs d'accès aux réseaux, Cisco Pix ou un routeur.

Cisco Secure ACS permet de s'assurer qu'un poste accédant au réseau est conforme aux politiques de sécurité du réseau.

Plusieurs vulnérabilités sont présentes sur Cisco Secure ACS :

- vulnérabilité CSCeb60017 et CSCec66913 : une vulnérabilité a été découverte dans l'interface d'administration CSAdmin, en écoute sur le port 2002/TCP. Elle permet à un utilisateur mal intentionné, par le biais d'un envoi répété de connexions de réaliser un déni de service sur l'équipement vulnérable. Les versions 3.2 et 3.2(2) build 15 sont affectées par cette vulnérabilité.
- vulnérabilité CSCec90317 : une vulnérabilité est présente sur Cisco Secure ACS en mode *proxy RADIUS*. Un utilisateur mal intentionné peut réaliser un déni de service par l'envoi de requêtes d'authentification. La version 3.2 est affectée par cette vulnérabilité ;
- vulnérabilité CSCed81716 : un utilisateur mal intentionné peut accéder à des données confidentielles, via l'utilisation d'un mot de passe vide, quand Cisco Secure ACS utilise une base de données NDS (Novell Directory Services) pour l'authentification des utilisateurs. Les versions ACS Solution Engine, Cisco ACS 3.2(3) et antérieures sont affectées par cette vulnérabilité.
- vulnérabilité CSCef05950 : un utilisateur mal intentionné peut, en usurpant l'adresse IP, voler la session d'un utilisateur déjà connecté à l'interface d'administration de Cisco Secure ACS. Les versions 3.2 et antérieures sont affectées par cette vulnérabilités.

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 ACS :

<http://www.cisco.com/warp/public/707/cisco-sa-20040825-ac.html>

Gestion détaillée du document

26 août 2004 version initiale.