



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 novembre 2004
N° CERTA-2004-AVI-359

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-359>

Gestion du document

Référence	CERTA-2004-AVI-359
Titre	Vulnérabilité dans Cisco Secure ACS
Date de la première version	04 novembre 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

- Elévation des privilèges ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Cisco Secure ACS Solution Engine versions 3.x antérieures à la version 3.3.2;
- Cisco Secure ACS versions 3.3.x antérieures à la version 3.3.2.

3 Résumé

Une vulnérabilité présente dans Cisco Secure ACS et Cisco Secure ACS Solution Engine permet à un utilisateur mal intentionné de contourner l'authentification.

4 Description

Une vulnérabilité due à un problème sur le traitement des certificats permet à un utilisateur mal intentionné, via l'utilisation d'un certificat malicieusement construit, de contourner l'authentification en mode EAP-TLS (Extensible Authentication Protocol Transport Layer Security).

5 Solution

Mettre à jour en appliquant le correctif disponible sur le site de l'éditeur ou remplacer la bibliothèque CSCRL . d11 corrigée.

6 Documentation

- Site internet Cisco :
<http://www.cisco.com>
- Bulletin de sécurité Cisco :
http://www.cisco.com/en/US/products/products_security_advisory09186a008033320e.shtml

Gestion détaillée du document

04 novembre 2004 version initiale.