



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 novembre 2004
N° CERTA-2004-AVI-367

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco Security Agent (CSA)

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-367>

Gestion du document

Référence	CERTA-2004-AVI-367
Titre	Vulnérabilité dans Cisco Security Agent (CSA)
Date de la première version	16 novembre 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Cisco du 11 novembre 2004
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco Security Agent versions 3.x ;
- Cisco Security Agent versions 4.x jusqu'à la version 4.0.3 build 728 ;
- Cisco Okena StormWatch versions 3.x.

3 Résumé

Une vulnérabilité présente dans les agents de sécurité Cisco Security Agent (CSA) permet à un utilisateur mal intentionné de contourner les règles de sécurité imposées par l'agent.

4 Description

Une vulnérabilité est présente dans le programme de protection des débordements de mémoire des agents de sécurité Cisco.

Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné via l'exploitation répétée d'un débordement de mémoire dans un faible intervalle de temps.

5 Solution

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

6 Documentation

- Site internet de Cisco :
<http://www.cisco.com>
- Bulletin de sécurité Cisco du 11 novembre 2004 :
<http://www.cisco.com/warp/public/707/cisco-sa-20041111-csa.shtml>

Gestion détaillée du document

16 novembre 2004 version initiale.