



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 septembre 2006
N° CERTA-2006-AVI-404

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité CISCO

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-2006-AVI-404>

Gestion du document

Référence	CERTA-2006-AVI-404
Titre	Vulnérabilité CISCO
Date de la première version	21 septembre 2006
Date de la dernière version	–
Source(s)	
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.

2 Systèmes affectés

- CISCO Guard Appliance versions 3.x ;
- CISCO Guard Appliance versions 5.0(3) ;
- CISCO Guard Appliance versions 5.1(5) ;
- CISCO Guard Blade versions 4.x ;

3 Résumé

Une vulnérabilité découverte dans CISCO Guard peut provoquer le contournement de la politique de sécurité au travers d'une attaque en `cross site scripting` (XSS).

4 Description

Le service CISCO Guard permettant éviter l'usurpation (spoofing) entre le client et le serveur web est vulnérable. La vulnérabilité peut être exploitée par un agresseur pour réaliser de l'injection de données ou encore rediriger l'utilisateur vers des sites malicieux.

5 Solution

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

6 Documentation

- Bulletins de sécurité de CISCO :
<http://cisco.com/warp/public/707/cisco-sa-20060920-guardxss.shtml>

Gestion détaillée du document

21 septembre 2006 version initiale.