

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité CISCO aux scans SSH

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-138>

Gestion du document

Référence	CERTA-2002-AVI-138
Titre	Vulnérabilité CISCO aux scans SSH
Date de la première version	28 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO : "Scanning for SSH Can Cause a Crach"
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.

2 Systèmes affectés

- Tous les équipements CISCO possédant une version d'IOS supportant le protocole SSH ;
- les commutateurs Catalyst 6000 fonctionnant avec CatOS ;
- les pare-feux PIX ;
- la famille des commutateurs CSS 11000.

3 Résumé

Une vulnérabilité présente dans le correctif fourni par CISCO pour corriger une vulnérabilité SSH sur certains équipements CISCO, permet à un individu mal intentionné d'effectuer un déni de service.

4 Description

Un correctif publié par CISCO afin de corriger certaines vulnérabilités SSH (Voir l'avis CERTA-2001-AVI-097 du CERTA) permet à un individu mal intentionné d'effectuer un déni de service. Effectivement, lors de l'envoi de paquets excessivement grands, le processus SSH va occuper une partie importante des cycles d'instructions du processeur causant un déni de service.

5 Solution

Appliquer les correctifs de CISCO selon les produits et leurs versions (cf. Documentation).

6 Documentation

Bulletin de sécurité CISCO "Scanning for SSH Can Cause Crash" :
<http://www.cisco.com/warp/public/707/SSH-scanning.shtml>

Avis CERTA-2001-AVI-097 du CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-097/>

Gestion détaillée du document

28 juin 2002 version initiale.