

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le service SSH des commutateurs CISCO 4000, 5000 ET 6000

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-2000-AVI-088>

Gestion du document

Référence	CERTA-2000-AVI-088
Titre	Vulnérabilité dans le service SSH des commutateurs CISCO 4000, 5000 ET 6000
Date de la première version	14 décembre 2000
Date de la dernière version	–
Source(s)	Avis 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

2 Systèmes affectés

Commutateurs CISCO Catalyst séries 4000, 5000 et 6000 possédant un IOS inférieur à la version 6.1(1c)

3 Résumé

Un utilisateur mal intentionné peut provoquer à distance un arrêt d'un commutateur CISCO (4000, 5000 ou 6000) par l'envoi de paquets « non attendus » sur le port SSH.

4 Description

Lorsqu'un paquet ne correspondant pas au protocole SSH est envoyé sur le port de ce service, une erreur est automatiquement générée. Cette erreur provoque un blocage du moteur de supervision du commutateur ayant pour effet un arrêt du traitement des paquets entrant et sortant.

Il peut entraîner également un redémarrage du système.

Nota : Par défaut la fonction SSH n'est pas mise en service et doit être configurée par l'administrateur.

5 Contournement provisoire

Désactiver le service SSH.

6 Solution

Appliquer la nouvelle version de l'IOS 6.1(1c) disponible sur le site :
<http://www.cisco.com>

7 Documentation

Avis de sécurité CISCO :
<http://www.cisco.com/warp/public/707/catalyst-ssh-protocolmismatch-pub.shtml>

Gestion détaillée du document

14 décembre 2000 version initiale.