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 2001
N° CERTA-2001-AVI-143

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les routeurs 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-2001-AVI-143

Gestion du document

Référence	CERTA-2001-AVI-143
Titre	Vulnérabilité dans les routeurs Cisco
Date de la première version	16 novembre 2001
Date de la dernière version	–
Source(s)	Bulletin 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

Dégradation des performances du routeur.

2 Systèmes affectés

Routeurs Cisco Series 12000.
Les autres produits Cisco ne sont pas affectés.

3 Résumé

La performance des routeurs Cisco de la série 12000 peut être dégradée lorsqu'ils doivent envoyer un grand nombre de paquets ICMP de type 3 *Destination Unreachable*. Cette situation peut se produire notamment lors de scans réseau très importants.

4 Description

La fonction d'un routeur est d'envoyer les paquets IP vers la bonne interface, en fonction de l'adresse destination incluse dans le paquet IP. Lorsqu'il n'y a pas de chemin valide vers la destination ou que le chemin valide est l'interface Null0, le paquet IP est écarté et le routeur envoie à son émetteur un paquet ICMP de type 3 *Destination Unreachable*.

Lorsqu'un nombre important de paquets IP est écarté par un routeur et nécessite l'envoi de beaucoup de réponses *Destination Unreachable*, les ressources du processeur du routeur peuvent être saturées.

Cette situation peut se produire lorsque le routeur est utilisé au milieu d'un mécanisme de filtrage *trou noir* (*), ou lorsqu'il est victime d'une attaque en déni de service.

(*) La méthode de filtrage *trou noir* au sein d'un réseau étendu consiste en l'annonce, par un routeur *trou noir*, de routes statiques d'adresses, dans le but de les filtrer. En effet, les paquets IP circulant sur ce réseau et possédant une des adresses destination concernées, arriveront jusqu'au routeur *trou noir*, où ils seront alors écartés.

5 Contournement provisoire

L'envoi de réponse *Destination Unreachable* peut être supprimé ou limité sur l'interface du routeur par les commandes suivantes :

- suppression : no ip unreachables
- limitation : ip icmp rate-limit unreachable n ou n est le nombre de millisecondes entre deux paquets ICMP *Destination Unreachable* consécutifs.

6 Solution

Cisco tient à disposition de ses clients un correctif pour éliminer cette vulnérabilité et leur conseille d'utiliser les canaux habituels de mise à jour et de maintenance.

7 Documentation

Avis Cisco :
http://www.cisco.com/warp/public/707/GSR-unreachables-pub.shtml

Gestion détaillée du document

16 novembre 2001 version initiale.