Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 avril 2002
N° CERTA-2002-AVI-083

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de la pile TCP/IP de FreeBSD

Gestion du document

Référence	CERTA-2002-AVI-083
Titre	Vulnérabilités de la pile TCP/IP de FreeBSD
Date de la première version	19 avril 2002
Date de la dernière version	–
Source(s)	Avis de sécurité FreeBSD-SA-02:20 Avis de sécurité FreeBSD-SA-02:21
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

- FreeBSD 4.5-RELEASE ;
- FreeBSD 4.4-STABLE ;
- FreeBSD 4.5-STABLE.

3 Résumé

Deux vulnérabilités découvertes dans la pile TCP/IP des systèmes FreeBSD peuvent être utilisées pour effectuer un déni de service.

4 Description

La première vulnérabilité concerne les mécanismes *syncache* et *syncookie*, qui servent à protéger le système d'une attaque de type *SYN flood*.

Une mauvaise gestion des pointeurs et des sockets liés à ces mécanismes peut provoquer l'arrêt brutal du système.

La deuxième vulnérabilité concerne la table de routage de la pile TCP/IP. A chaque nouvelle connexion TCP avec un hôte distant, une entrée est ajoutée dans cette table, avec un compteur indiquant le nombre de connexions en cours. Lorsque ce compteur est à zéro, l'entrée est effacée de la table.

Une erreur de la fonction *ip_output()* lors d'un message de type *ICMP echo reply* provoque l'incrémentation d'une éventuelle entrée de la table, ce qui peut amener à une saturation de la mémoire du système.

Cette vulnérabilité peut être exploitée par un utilisateur distant mal intentionné pour effectuer un déni de service sur le système.

5 Solution

Mettre à jour la version de FreeBSD.

6 Documentation

Avis de sécurité FreeBSD-SA-02:20 :
ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:20.syncache.asc

Avid de sécurité FreeBSD-SA-02:21 :
ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:21.tcpip.asc

Gestion détaillée du document

19 avril 2002 version initiale.