

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités FreeBSD (ipfw)

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-2005-AVI-240>

Gestion du document

Référence	CERTA-2005-AVI-240
Titre	Vulnérabilités FreeBSD (ipfw)
Date de la première version	01 juillet 2005
Date de la dernière version	–
Source(s)	Mise à jour de sécurité de l'éditeur du 29 juin 2006
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

Mauvaise application des règles de filtrage.

2 Systèmes affectés

FreeBSD dans sa version 5.4 sur les architectures multi-processeurs (Symetric Multi-Processor : SMP) ou bien sur les architectures mono-processeur (Uni Processor : UP) avec l'option noyau préemptif (PREEMPTION kernel).

3 Résumé

ipfw(8) est un des systèmes de filtrage installé nativement dans FreeBSD. Il permet le filtrage de paquets IP, leur redirection ainsi que la gestion du trafic. La commande `ipfw lookup tables` permet de spécifier efficacement de nombreuses adresses IP qui pourront être exploitées lors du contrôle de paquets.

4 Description

La vulnérabilité permet à un utilisateur malveillant de modifier une adresse IP mise en cache. Ainsi, un paquet pourrait être traité contrairement aux règles de filtrage définies dans la politique de sécurité.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). En attendant l'application des directives de l'éditeur, il est possible de se protéger en interdisant l'usage de la commande `lookup tables`.

6 Documentation

- Bulletin de sécurité de FreeBSD du 29 juin 2005 :
<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:13.ipfw.asc>
- Références CVE CAN-2005-2019 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2019>

Gestion détaillée du document

01 juillet 2005 version initiale.