

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du système de filtrage pf

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-2006-AVI-045>

Gestion du document

Référence	CERTA-2006-AVI-045
Titre	Vulnérabilité du système de filtrage pf
Date de la première version	25 janvier 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD FreeBSD-SA-06:07.pf du 25 janvier 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

Déni de service à distance.

2 Systèmes affectés

- FreeBSD 5.3 ;
- FreeBSD 5.4 ;
- FreeBSD 6.0.

3 Résumé

Une vulnérabilité dans le système de filtrage pf (`packet filter`) permet à un utilisateur mal intentionné de créer un déni de service sur la plate-forme vulnérable.

4 Description

pf (`packet filter`) est un système de filtrage utilisé initialement sous le système d'exploitation OpenBSD puis porté sur différents systèmes d'exploitation.

Une vulnérabilité dans la gestion du cache des paquets IP fragmentés permet à un utilisateur distant mal intentionné, via une séquence de paquets IP malicieuse, de créer un déni de service sur la plate-forme vulnérable en provoquant l'arrêt brutal de la machine.

5 Contournement provisoire

Ne pas utiliser les directives `scrub fragment crop` ou `scrub fragment drop-ovl` mais plutôt `scrub fragment reassemble`.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité FreeBSD SA-06:07.pf du 25 janvier 2006 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:07.pf.asc>

Gestion détaillée du document

25 janvier 2006 version initiale.