



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 01 février 2002  
N° CERTA-2002-AVI-021-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Mise à jour de la gestion des fragments dans *Ipfiler*

---

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-2002-AVI-021>

---

### Gestion du document

Référence	CERTA-2002-AVI-021-001
Titre	Mise à jour de la gestion des fragments dans <i>Ipfiler</i>
Date de la première version	01 février 2002
Date de la dernière version	06 mars 2002
Source(s)	Base de vulnérabilités BugTraq
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

Contournement des règles de filtrage de paquets implémentées par *Ipfiler*.

## 2 Systèmes affectés

- Versions d'*Ipfiler* 3.4.16 et inférieures
- HP-UX 11.00 et 11.11
- FreeBSD 4.2 et inférieures
- NetBSD 1.5 et inférieures
- OpenBSD 2.8 et inférieures

## 3 Résumé

*Ipfiler* est une collection d'outils de filtrage de paquets répandue dans le monde *Unix*. Une vulnérabilité permet d'accéder aux ports normalement bloqués des hôtes protégés par le pare-feu.

## 4 Description

Le cache de gestion des fragments a pour objet de laisser passer les fragments d'un paquet IP correspondant à une session/connexion précédemment acceptée par le module de filtrage. Hors, ce cache ne se base que sur l'entête IP,

il est alors possible, après avoir initié une connexion autorisée, d'envoyer des fragments vers des ports arbitraires.

## 5 Solution

Mettre à jour les sources ou le paquetage, selon les vendeurs :

- Sources d'*Ipfilter* :  
<ftp://coombs.anu.edu.au/pub/net/ip-filter/>
- HP-UX :  
[http://www.software.hp.com/cgi-bin/swdepot\\_parser.cgi/cgi/displayProductInfo.pl?productNumber=B9901AA](http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B9901AA)
- FreeBSD :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-01:32/ipfilter.patch>
- NetBSD : se conformer à l'avis cité dans la documentation.
- OpenBSD 2.8 voir :  
[http://www.openbsd.org/errata28.html#ipf\\_frag](http://www.openbsd.org/errata28.html#ipf_frag)

## 6 Documentation

- Base de vulnérabilités Bugtraq  
<http://www.securityfocus.com/bid/2545>
- Avis de sécurité NetBSD  
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2001-007.txt.asc>
- Avis de sécurité FreeBSD  
<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:32.ipfilter.v1.1.asc>

## Gestion détaillée du document

**01 février 2002** version initiale.

**06 mars 2002** correction d'un lien défectueux.