



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 mai 2002
N° CERTA-2002-AVI-093

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de /dev/ipfilter sous IRIX

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-093>

Gestion du document

Référence	CERTA-2002-AVI-093
Titre	Vulnérabilité de /dev/ipfilter sous IRIX
Date de la première version	02 mai 2002
Date de la dernière version	–
Source(s)	Avis de sécurité IRIX 20020408-01-I
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

Système IRIX versions 6.5 à 6.5.10.
Les versions antérieures, non maintenues, n'ont pas été testées.

3 Résumé

Les droits d'accès au fichier /dev/ipfilter sont trop permissifs et permettent à un utilisateur mal intentionné de provoquer un déni de service.

4 Description

Le fichier /dev/ipfilter est créé par défaut sur les systèmes IRIX 6.5 pendant l'installation. Ce fichier est utilisé par le service ipfilterd du paquetage eoe.sw.ipgate pour le filtrage du trafic IP.

Les droits par défaut sur ce fichier sont 0x644, et permettent à un utilisateur non privilégié de perturber le trafic IP.

5 Contournement provisoire

Modifier les droits du fichier `/dev/ipfilter` :

```
# chmod 600 /dev/ipfilter
```

Attention : le script `/dev/MAKEDEV` repositionne les droits à 0x644 chaque fois qu'il est exécuté.

6 Solution

La version IRIX 6.5.11 et les versions suivantes corrigent le problème.

7 Documentation

Avis de sécurité SGI 20020408-01-I :

<ftp://patches.sgi.com/support/free/security/advisories/20020408-01-I>

Gestion détaillée du document

02 mai 2002 version initiale.