



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 octobre 2003
N° CERTA-2003-AVI-161

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans procfs et linprocfs sous FreeBSD

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-2003-AVI-161>

Gestion du document

Référence	CERTA-2003-AVI-161
Titre	Vulnérabilité dans procfs et linprocfs sous FreeBSD
Date de la première version	10 octobre 2003
Date de la dernière version	–
Source(s)	Avis PINE-CERT-20030902 de Pine Digital Security Avis FreeBSD-SA-03:17.procfs de FreeBSD
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

- Fuite d'informations ;
- déni de service.

2 Systèmes affectés

Toutes les versions de FreeBSD.

3 Résumé

Un problème dans la mise en œuvre des systèmes de fichiers spéciaux `procfs` et `linprocfs` sous FreeBSD a été découvert.

4 Description

`Procfs` est un système de fichiers spéciaux permettant d'obtenir une vue hiérarchique de la table des processus à travers le système de fichier (`/proc`). `Linprocfs` est la mise en oeuvre d'un sous-système de fichiers sous FreeBSD nécessaire à l'exécution des binaires Linux.

Une faille dans le contrôle de certains champs de la structure `uio` utilisée dans le traitement des requêtes de ces systèmes de fichiers permet à un utilisateur mal intentionné d'effectuer un déni de service ou d'obtenir des informations présentes dans une partie de la mémoire du noyau.

5 Solution

Mettre à jour les systèmes vulnérables avec les correctifs disponibles (cf. Documentation).

6 Documentation

Bulletin de sécurité #FreeBSD-SA-03:17.procfs de FreeBSD :

<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:17.procfs.asc>

Bulletin de sécurité #PINE-CERT-20030902 de Pine Digital Security :

<http://www.pine.nl/press/pine-cert-20030902.txt>

Gestion détaillée du document

10 octobre 2003 version initiale.