



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 05 janvier 2006  
N° CERTA-2006-AVI-010

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le gestion de /dev/fd de OpenBSD

---

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-010>

---

### Gestion du document

Référence	CERTA-2006-AVI-010
Titre	Vulnérabilité dans le gestion de /dev/fd de OpenBSD
Date de la première version	05 janvier 2006
Date de la dernière version	–
Source(s)	Liste des mises à jour OpenBSD
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

OpenBSD versions 3.7 et 3.8.

## 3 Résumé

Une vulnérabilité dans le gestion de /dev/fd permet de contourner de la politique de sécurité.

## 4 Description

Une vulnérabilité a été découverte dans la gestion de /dev/fd. Cette vulnérabilité peut être exploitée par un utilisateur mal-intentionné afin de taper des programmes `suid` et ainsi, contourner la politique de sécurité ou procéder à une élévation de privilèges.

## **5 Solution**

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

## **6 Documentation**

- Liste des correctifs de sécurité OpenBSD pour fd du 05 janvier 2006 :  
<http://openbsd.org/errata37.html#fd>
- Correctif de sécurité pour les version 3.7 et 3.8 :  
[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.7/common/008\\_fd.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.7/common/008_fd.patch)  
[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.8/common/002\\_fd.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.8/common/002_fd.patch)

## **Gestion détaillée du document**

**05 janvier 2006** version initiale.