

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de ptrace dans les systèmes BSD

---

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-016>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2002-AVI-016                            |
| Titre                       | Vulnérabilité de ptrace dans les systèmes BSD |
| Date de la première version | 28 janvier 2002                               |
| Date de la dernière version | –   |
| Source(s)                   | Avis de sécurité NetBSD 2002-001              |
| 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

Elévation de privilèges.

## 2 Systèmes affectés

- NetBSD 1.5.x versions 1.5.2 et antérieures ;
- NetBSD 1.4.x versions 1.4.3 et antérieures ;
- OpenBSD version 3.0 ;
- FreeBSD versions 4.4 et antérieures.

## 3 Résumé

Un utilisateur mal intentionné peut, en local, obtenir les droits de l'utilisateur *root* en utilisant la fonction *ptrace*.

## 4 Description

La commande *ptrace* est une fonction de débogage qui permet de contrôler l'exécution d'un processus fils, et d'éditer son image mémoire. Il y a des restrictions sur son utilisation avec des processus ayant le drapeau *SUID* ou *SGID* activé.

Une vulnérabilité de ces contrôles dans les noyaux BSD permet à un utilisateur mal intentionné d'obtenir les droits de l'utilisateur *root*.

## 5 Solution

Appliquer les correctifs des éditeurs (cf. Documentation).

## 6 Documentation

- Avis de sécurité FreeBSD SA-02-08 :  
<http://www.freebsd.org/security/index.html>
- Avis de sécurité NetBSD SA-2002-001 :  
<http://www.netbsd.org/Security/>
- Avis de sécurité OpenBSD :  
<http://www.openbsd.org/security.html>

## Gestion détaillée du document

28 janvier 2002 version initiale.