

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de shmat sur les noyaux 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-2004-AVI-023>

---

### Gestion du document

Référence	CERTA-2004-AVI-023-001
Titre	Vulnérabilité de shmat sur les noyaux BSD
Date de la première version	06 février 2004
Date de la dernière version	19 février 2004
Source(s)	Bulletin de sécurité PINE-CERT-20040201 de Pine Digital Security Bulletin de sécurité FreeBSD-SA-04:02.shmat 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

Elévation de privilèges.

## 2 Systèmes affectés

- FreeBSD 5.2 et versions antérieures, FreeBSD 4.9 et versions antérieures ;
- OpenBSD 3.4 et versions antérieures.

## 3 Résumé

Une vulnérabilité présente dans la fonction `shmat()` présente dans les noyaux de souche BSD peut être exploitée par un utilisateur mal intentionné pour réaliser une élévation de privilèges.

## 4 Description

`shmat()` permet d'inclure un segment de mémoire partagée dans l'espace d'adressage d'un processus.

Une vulnérabilité est présente dans la fonction `shmat ( )` (problème dans la gestion des références à un segment de mémoire partagée). Un utilisateur local peut exploiter cette vulnérabilité pour réaliser une élévation de privilèges et obtenir les droits du super-utilisateur `root` sur la plate-forme vulnérable.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs :

- Bulletin de sécurité FreeBSD-SA-04:02.shmat de FreeBSD :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:02.shmat.asc>
- Bulletin de sécurité d'OpenBSD :  
<http://www.openbsd.org/errata.html#sysvshm>
- Bulletin de sécurité de NetBSD :  
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-004.txt.asc>

## 6 Documentation

- Bulletin de sécurité PINE-CERT-20040201 de Pine Digital Security :  
<http://www.pine.nl/press/pine-cert-20040201.txt>
- Référence CVE CAN-2004-0114 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0114>

## Gestion détaillée du document

**06 février 2004** version initiale.

**19 février 2004** Ajout référence au bulletin de sécurité de NetBSD.