

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de la fonction `realpath` pour 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-2003-AVI-134>

---

### Gestion du document

Référence	CERTA-2003-AVI-134-001
Titre	Vulnérabilité de la fonction <code>realpath</code> pour les systèmes BSD
Date de la première version	06 août 2003
Date de la dernière version	18 août 2003
Source(s)	Avis de sécurité 2003-011 de NetBSD Avis de sécurité FreeBSD-SA-03:08 de FreeBSD Avis de sécurité d'OpenBSD Note VU#743092 du CERT/CC
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 ;
- exécution de code arbitraire à distance ;
- déni de service.

## 2 Systèmes affectés

- OpenBSD 3.3 et versions antérieures ;
- FreeBSD 5.0, FreeBSD 4.8 et versions antérieures ;
- NetBSD 1.6.1 et versions antérieures ;
- Versions de Mac OS X antérieures à 10.2.6.

### 3 Description

Une vulnérabilité de type débordement de mémoire est présente dans la fonction `realpath()` de la bibliothèque standard C (`libc`) sur différents systèmes d'exploitation de souche BSD (FreeBSD, NetBSD, OpenBSD, Mac OS X).

Cette vulnérabilité peut être exploitée au travers d'applications utilisant cette fonction, comme le service ftp (`ftpd`), pour réaliser une exécution de code arbitraire pouvant entraîner une élévation de privilèges ou un déni de service.

### 4 Solution

Appliquer le correctif de l'éditeur :

- Bulletin de sécurité FreeBSD-SA-03-08 de FreeBSD :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:08.realpath.asc>
- Bulletin de sécurité NetBSD-SA2003-011 de NetBSD :  
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-011.txt.asc>
- Bulletin de sécurité d'OpenBSD :  
<http://www.openbsd.org/errata.html#realpath>
- Bulletin de sécurité d'Apple pour Mac OS X Server :  
<http://docs.info.apple.com/article.html?artnum=120238>
- Bulletin de sécurité d'Apple pour Mac OS X Client :  
<http://docs.info.apple.com/article.html?artnum=120239>

### 5 Documentation

- Référence CVE CAN-2003-0466 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0466>
- Note VU#743092 du CERT/CC :  
<http://www.kb.cert.org/vuls/id/743092>

### Gestion détaillée du document

**06 août 2003** version initiale.

**18 août 2003** ajout références aux bulletins de sécurité d'Apple pour Mac OS X.