

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples Vulnérabilités de 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-2009-AVI-425>

---

### Gestion du document

Référence	CERTA-2009-AVI-425
Titre	Multiples vulnérabilités de FreeBSD
Date de la première version	07 octobre 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité FreeBSD du 02 octobre 2009
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 ;
- déni de service.

## 2 Systèmes affectés

- FreeBSD version 6.3 ;
- FreeBSD version 6.4 ;
- FreeBSD version 7.1 ;
- FreeBSD version 7.2.

## 3 Résumé

Deux vulnérabilités présentes dans FreeBSD permettent à un utilisateur local de provoquer un déni de service ou d'exécuter du code arbitraire avec des droits élevés.

## 4 Description

Deux vulnérabilités sont présentes dans FreeBSD :

- la première est relative à la mise en œuvre des tubes (*pipe*) et permet à un utilisateur local de provoquer un déni de service ou d'exécuter du code arbitraire dans le contexte du noyau. Cette vulnérabilité ne touche que les versions 6.x de FreeBSD ;
- la seconde vulnérabilité touche le composant `devfs` (`device file system`) et permet à un utilisateur local de provoquer un déni de service ou d'exécuter du code arbitraire dans le contexte du noyau.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité FreeBSD SA-09:13.pipe du 02 octobre 2009 :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-09:13.pipe.asc>
- Bulletin de sécurité FreeBSD SA-09:14.devfs du 02 octobre 2009 :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-09:14.devfs.asc>

## Gestion détaillée du document

**07 octobre 2009** version initiale.