



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 07 octobre 2008  
N° CERTA-2008-AVI-461-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-2008-AVI-461>

---

### Gestion du document

Référence	CERTA-2008-AVI-461-001
Titre	Vulnérabilité de FreeBSD
Date de la première version	16 septembre 2008
Date de la dernière version	07 octobre 2008
Source(s)	Bulletin de sécurité FreeBSD-SA-08:09.icmp6
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

Déni de service à distance.

## 2 Systèmes affectés

- FreeBSD 6.3 ;
- FreeBSD 7.0.

## 3 Résumé

Une vulnérabilité présente dans le noyau de FreeBSD permet à un utilisateur distant de provoquer un déni de service du système vulnérable.

## 4 Description

Une erreur est présente dans la pile IPv6 des systèmes FreeBSD. Celle-ci est relative à la gestion des paquets de type ICMPv6 et permet à un utilisateur distant de provoquer un déni de service par le biais d'un paquet ICMPv6 construit de façon particulière.

Le fait que la pile IPv6 soit active sur le système n'est pas suffisant pour exploiter la vulnérabilité. Il est nécessaire qu'une *socket* TCP IPv6 soit en écoute sur l'interface par laquelle seront reçus les paquets de l'attaquant.

## 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-08:09.icmp6 du 03 septembre 2008 :  
<http://security.freebsd.org/FreeBSD-SA-08:09.icmp6.asc>
- Référence CVE CVE-2008-3530 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-3530>

## Gestion détaillée du document

**16 septembre 2008** version initiale.

**07 octobre 2008** ajout de la référence CVE.