

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de la fonction `setsockopt()` sous 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-2004-AVI-105>

---

### Gestion du document

Référence	CERTA-2004-AVI-105
Titre	Vulnérabilité de la fonction <code>setsockopt()</code> sous FreeBSD
Date de la première version	30 mars 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD-SA-04-06.ipv6 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

- Déni de service ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

FreeBSD 5.2-RELEASE et versions antérieures.

## 3 Résumé

Une vulnérabilité dans la fonction `setsockopt()` peut être exploitée par un utilisateur local mal intentionné afin de provoquer un déni de service ou accéder à des données du noyau.

## 4 Description

La fonction `setsockopt()` permet de manipuler les options associées à une `socket`.

Une vulnérabilité présente dans la gestion des options pour une `socket` IPv6 peut être exploitée par un utilisateur local mal intentionné afin de provoquer un déni de service par arrêt brutal du système. Il serait également possible d'exploiter cette vulnérabilité afin de lire certaines portions de la mémoire du noyau.

## **5 Contournement provisoire**

Désactiver la prise en compte du protocole IPv6 au niveau du noyau (pour plus d'informations se référer au bulletin de sécurité de l'éditeur).

## **6 Solution**

Appliquer les correctifs (se référer au bulletin de sécurité de l'éditeur).  
La version 5.2.1-RELEASE-p4 corrige cette vulnérabilité.

## **7 Documentation**

- Bulletin de sécurité FreeBSD-SA-04:06.ipv6 de FreeBSD :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:06.ipv6.asc>
- Référence CVE CAN-2004-0370 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0370>

## **Gestion détaillée du document**

**30 mars 2004** version initiale.