

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du noyau 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-2006-AVI-044>

Gestion du document

Référence	CERTA-2006-AVI-044
Titre	Vulnérabilités du noyau de FreeBSD
Date de la première version	25 janvier 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD SA-06:06.kmem du 25 janvier 2006
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

Atteinte à la confidentialité des données.

2 Systèmes affectés

- FreeBSD 5.4 ;
- FreeBSD 6.0.

3 Résumé

Deux vulnérabilités du noyau de FreeBSD permettent à un utilisateur local mal intentionné de porter atteinte à la confidentialité des données.

4 Description

Deux vulnérabilités sont présentes dans le noyau FreeBSD :

- la première est due à une erreur dans l'initialisation d'un tampon présent dans la pile du noyau FreeBSD (CVE-2006-379) qui, lorsqu'il est consulté par le biais d'un appel système, peut encore contenir des données sensibles appartenant à d'autres utilisateurs ;

- la deuxième vulnérabilité est due à erreur dans le calcul de la taille d'un tampon par le noyau FreeBSD (CVE-2006-380). Elle permet à un utilisateur local mal intentionné d'avoir accès à des zones de la pile en dehors de ce tampon et contenant potentiellement des informations sensibles. Dans les deux cas, ces vulnérabilités permettent à un utilisateur local mal intentionné de porter atteinte à la confidentialité des données en réalisant un appel système.

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-06:06 du 25 janvier 2006 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:06.kmem.asc>
- Référence CVE CAN-2006-0379 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0379>
- Référence CVE CAN-2006-0380 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0380>

Gestion détaillée du document

25 janvier 2006 version initiale.