

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-229>

Gestion du document

Référence	CERTA-2009-AVI-229
Titre	Vulnérabilités dans FreeBSD
Date de la première version	11 juin 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité FreeBSD SA-09:09.pipe et SA-09:10.ipv6 du 10 juin 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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- FreeBSD 6.x ;
- FreeBSD 7.1.

3 Résumé

Deux vulnérabilités ont été découvertes dans FreeBSD et permettent à une personne malveillante de contourner la politique de sécurité et de porter atteinte à la confidentialité des données.

4 Description

Plusieurs vulnérabilités ont été découvertes dans `FreeBSD` :

- la première affecte la commande *pipe* et permet à un processus de lire des pages de la mémoire appartenant à un autre processus ou au noyau ;
- la seconde concerne l'implémentation du protocole *IPv6* et permet à un utilisateur d'accéder à des propriétés d'une interface *IPv6* ou de la désactiver.

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-09:09.pipe du 10 juin 2009 :
<http://security.freebsd.org/advisories/FreeBSD-SA-09:09.pipe.asc>
- Bulletin de sécurité FreeBSD SA-09:10.ipv6 du 11 juin 2009 :
<http://security.freebsd.org/advisories/FreeBSD-SA-09:10.ipv6.asc>

Gestion détaillée du document

11 juin 2009 version initiale.