

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-2008-AVI-020>

Gestion du document

Référence	CERTA-2008-AVI-020
Titre	Multiples vulnérabilités de FreeBSD
Date de la première version	15 janvier 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité FreeBSD du 14 janvier 2008
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

- Exécution de code arbitraire à distance ;
- déni de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

FreeBSD 6.x.

3 Résumé

De multiples vulnérabilités affectent FreeBSD. Ces vulnérabilités peuvent être exploitées afin d'exécuter des commandes arbitraires à distance ou accéder à des informations sensibles en local.

4 Description

Trois vulnérabilités ont été découvertes dans FreeBSD :

- la première résulte d'une erreur de gestion de limite de boucle (*off-by-one*) au niveau de la fonction `inet_network()`. Cette vulnérabilité peut être exploitée à distance par un utilisateur malintentionné afin d'exécuter du code ;

- la seconde est due à une erreur dans la fonction `openpty()`. Cette vulnérabilité peut être exploitée en local afin d'accéder à des informations confidentielles pour un utilisateur standard ;
- enfin, la dernière vulnérabilité est due à une erreur dans le fonction `ptsname()`. Cette vulnérabilité peut être exploitée en local afin de devenir propriétaire d'un `pty` à accès restreint.

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-08:01.pty du 14 janvier 2008 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-08:01.pty.asc>
- Bulletin de sécurité FreeBSD SA-08:02.libc du 14 janvier 2008 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-08:02.libc.asc>
- Référence CVE CVE-2008-0216 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0216>
- Référence CVE CVE-2008-0217 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0217>
- Référence CVE CVE-2008-0122 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0122>

Gestion détaillée du document

15 janvier 2008 version initiale.