Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 décembre 2007
N° CERTA-2007-AVI-525

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans FreeBSD

Gestion du document

Référence	CERTA-2007-AVI-525
Titre	Vulnérabilité dans FreeBSD
Date de la première version	06 décembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD SA-07:09.random
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.

2 Systèmes affectés

- FreeBSD versions 5.5 et antérieures ;
- FreeBSD versions 6.2 et antérieures.

3 Résumé

Une vulnérabilité dans `FreeBSD` permet à un utilisateur de contourner la politique de sécurité du système.

4 Description

Une vulnérabilité dans le générateur d'aléa de `FreeBSD` mis en œuvre par les périphériques */dev/random* et */dev/urandom* permet à un utilisateur malveillant, dans certaines circonstances, de tirer à nouveau le même aléa de façon prédictible. Ceci pourrait mettre en défaut les applications se basant sur cet aléa pour effectuer des opérations de chiffrement ou de hâchage.

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-07:09.random du 29 novembre 2007 :
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-07:09.random.asc

Gestion détaillée du document

06 décembre 2007 version initiale.