

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans la fonction "readv" 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-2003-AVI-162>

Gestion du document

Référence	CERTA-2003-AVI-162-001
Titre	Vulnérabilités dans la fonction "readv" sous FreeBSD
Date de la première version	10 octobre 2003
Date de la dernière version	17 octobre 2003
Source(s)	Avis de sécurité de Pine Digital PINE-CERT-20030901 Avis de sécurité FreeBSD SA-03:16
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 ;
- élévation de privilèges.

2 Systèmes affectés

FreeBSD versions 4.3 à 4.8 incluses.
Les versions 5.x ne sont pas vulnérables.

3 Résumé

Deux vulnérabilités de la fonction "readv" permettent à un utilisateur local mal intentionné de provoquer un déni de service ou d'obtenir les droits en lecture et en écriture sur des fichiers du système.

4 Description

La fonction "*readv*" lit le contenu d'un descripteur de fichier et place les données dans des mémoires tampons.

Une première vulnérabilité permet à un utilisateur mal intentionné de provoquer l'arrêt brutal du serveur en appelant la fonction "*readv*" un grand nombre de fois, puis en fermant le descripteur de fichier.

Une seconde vulnérabilité permet à un utilisateur d'obtenir les droits en lecture ou en écriture sur un fichier du système. En effet, un descripteur de fichier peut pointer vers une zone de mémoire non allouée tout en restant valide. Si un fichier est alors créé dans cette zone de mémoire, un utilisateur peut obtenir un accès en lecture ou en écriture au fichier nouvellement créé.

5 Solution

Appliquer le correctif disponible sur le site de FreeBSD (cf. section Documentation).

6 Documentation

Avis de sécurité de Pine Digital PINE-CERT-20030901 :
<http://www.pine.nl/press/pine-cert-20030901.txt>

Avis de sécurité FreeBSD FreeBSD-SA-03:16 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:16.filedesc.asc>

Gestion détaillée du document

10 octobre 2003 version initiale.

17 octobre 2003 première modification : correction du lien de l'avis de Pine Digital.