

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Problème de gestion des descripteurs de fichier sous BSD

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-2002-AVI-167>

Gestion du document

Référence	CERTA-2002-AVI-167
Titre	Problème de gestion des descripteurs de fichier sous BSD
Date de la première version	05 août 2002
Date de la dernière version	–
Source(s)	Avis FreeBSD-SA-02:23.stdio
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

Elévation de privilèges.

2 Systèmes affectés

- Toutes les versions de FreeBSD antérieures à la version 4 . 6-RELEASE (inclusive).
La version 4 . 6-STABLE (avant la correction du 30 juillet 2002) est également vulnérable.
- Toutes les versions de OpenBSD antérieures à la version 3 . 1 (inclusive).

3 Résumé

Une mauvaise gestion des descripteurs de fichier sous FreeBSD permet à un utilisateur mal intentionné d'élever ses privilèges.

4 Description

Par convention, sur les systèmes POSIX, les descripteurs de fichier 0, 1 et 2 correspondent respectivement à l'entrée standard, la sortie standard et l'erreur standard.

Les descripteurs de fichier sont alloués séquentiellement, en partant du numéro de descripteur non attribué le plus bas. Si un programme `set-uid` ou `set-gid` était lancé avec certains descripteurs d'entrée/sortie fermés (descripteurs 0, 1 et 2), ce programme pourrait ouvrir un fichier et l'associer par erreur à l'entrée standard, la sortie standard ou l'erreur standard. Le programme pourrait ainsi lire des données d'un fichier, ou écrire dans celui-ci par erreur.

L'exploitation de cette vulnérabilité permet, dans certains cas, à un utilisateur local mal intentionné d'obtenir les privilèges `root`.

5 Solution

Mettre à jour le noyau. Se référer aux avis de sécurité du distributeur.

6 Documentation

Avis de sécurité FreeBSD-SA-02:23.stdio :

<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:23.asc>

Avis de sécurité OpenBSD `fdalloc2` du 8 mai 2002 :

<http://www.openbsd.org/errata.html>

Gestion détaillée du document

05 août 2002 version initiale.