

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur jail_attach 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-2004-AVI-057>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2004-AVI-057 |
| Titre | Vulnérabilité sur jail_attach sous FreeBSD |
| Date de la première version | 01 mars 2004 |
| Date de la dernière version | – |
| Source(s) | Avis de sécurité FreeBSD (FreeBSD-SA-04:03.jail) |
| 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 des privilèges.

2 Systèmes affectés

- FreeBSD 5.1-Release ;
- FreeBSD 5.2-Release.

3 Résumé

Une vulnérabilité présente dans la primitive système jail_attach permet à un utilisateur mal intentionné dans un environnement d'exécution restreint d'utiliser un autre environnement d'exécution restreint.

4 Description

La commande jail, une extension de la primitive chroot sous Unix, permet à un processus de s'exécuter dans un environnement restreint.

La primitive système `jail_attach` permet de faire passer un processus d'un environnement non restreint vers un environnement restreint.

Une vulnérabilité présente dans cette fonction permet à un processus s'exécutant dans un environnement restreint de pouvoir s'exécuter dans un autre environnement restreint sans contrôle des privilèges du premier processus.

5 Solution

Appliquer le correctif correspondant à votre version (cf. section documentation).

6 Documentation

- Avis de sécurité FreeBSD :
<http://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:03.jail.asc>
- Correctif disponible à l'adresse suivante :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-04:03/jail.patch>

Gestion détaillée du document

01 mars 2004 version initiale.