Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mai 2004
N° CERTA-2004-AVI-176

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la primitive système msync de FreeBSD

Gestion du document

Référence	CERTA-2004-AVI-176
Titre	Vulnérabilité de la primitive système msync de FreeBSD
Date de la première version	27 mai 2004
Date de la dernière version	–
Source(s)	Avis de sécurité FreeBSD FreeBSD-SA-04:11.msync
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

Atteinte à l'intégrité des données.

2 Systèmes affectés

- FreeBSD 4.8, 4.9 et 4.10 ;
- FreeBSD 5.2.

3 Résumé

Une vulnérabilité dans FreeBSD permet à un utilisateur mal intentionné de porter atteinte à l'intégrité des données.

4 Description

La primitive système `msync()` permet aux applications de demander l'écriture de pages mémoires modifiées sur le disque. Des erreurs de programmation de cette fonction peuvent conduire à une corruption du cache entre la mémoire virtuelle et le contenu du disque. Cette vulnérabilité peut être utilisée par un utilisateur mal intentionné

afin de porter atteinte à l'intégrité des données (empêcher les changements effectués sur un fichier d'être écrits sur le disque).

5 Solution

Appliquer le correctif fourni par FreeBSD.

- Pour FreeBSD 5.2 :
  ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:11/msync5.patch
- Pour FreeBSD 4.8, 4.9 et 4.10 :
  ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:11/msync4.patch

6 Documentation

- Avis de sécurité FreeBSD FreeBSD-SA-04:11.msync du 26 mai 2004 :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:11.msync.asc
- Référence CVE CAN-2004-0435 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0435

Gestion détaillée du document

27 mai 2004 version initiale.