Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 novembre 2003
N° CERTA-2003-AVI-198

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du noyau OpenBSD

Gestion du document

Référence	CERTA-2003-AVI-198
Titre	Multiples vulnérabilités du noyau OpenBSD
Date de la première version	24 novembre 2003
Date de la dernière version	–
Source(s)	Bulletins de sécurité d'OpenBSD
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 ;
- déni de service.

2 Systèmes affectés

OpenBSD 3.4 et versions antérieures.

3 Description

Une vulnérabilité de type débordement de mémoire est présente dans le module `compat_ibcs2` du noyau OpenBSD.

Au moyen d'un fichier `COFF` habilement constitué, un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'obtenir les privilèges du super-utilisateur `root` ou réaliser un déni de service par arrêt brutal du système.

De plus, deux primitives système (`sysctl` et `semop/semctl`) présentant une vulnérabilité (mauvais contrôle des paramètres en entrée pouvant entraîner un débordement de mémoire) ont fait l'objet d'un correctif.

L'ensemble de ces vulnérabilités n'est pas exploitable à distance.

4 Solution

Se référer aux bulletins de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

5 Documentation

- Bulletin de sécurité relatif à `compat_ibcs2` :
  http://www.openbsd.org/errata.html#ibcs2
- Correctif relatif à `semop/semctl` :
  http://www.openbsd.org/errata.html#sem
- Correctif relatif à `sysctl` :
  http://www.openbsd.org/errata.html#uvm

Gestion détaillée du document

24 novembre 2003 version initiale.