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 mars 2003
N° CERTA-2003-AVI-038-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la commande file

Gestion du document

Référence	CERTA-2003-AVI-038-003
Titre	Vulnérabilité de la commande file
Date de la première version	10 mars 2003
Date de la dernière version	24 mars 2003
Source(s)	Bulletin de sécurité 03.04.03 de iDEFENSE
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

Exécution de code arbitraire.

2 Systèmes affectés

Les versions de `file` antérieures à 3.41 sont vulnérables.
La version 3.41 de `file` corrige cette vulnérabilité.

3 Résumé

Une vulnérabilité de type débordement de mémoire est présente dans la commande `file`.

4 Description

La commande `file` présente sur de nombreux systèmes Unix/Linux est utilisée pour déterminer le type d'un fichier.

Une vulnérabilité de type débordement de mémoire est présente dans la routine de traitement des en-têtes de fichiers ELF (Executable and Linking Format).

En utilisant la commande `file` pour déterminer le type d'un fichier habilement constitué, un utilisateur peut déclencher l'exécution d'un code arbitraire contenu dans ce fichier.

5 Solution

Appliquer le correctif fourni par l'éditeur (Cf. section Documentation).

6 Documentation

- Bulletin de sécurité 03.04.03 "Locally exploitable buffer overflow in file" d'iDEFENSE : http://www.idefense.com/advisory/03.04.03.txt
- Bulletin de sécurité MDKSA-2003:030 de Mandrake : http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:030
- Bulletin de sécurité RHSA-2003:086 de Red Hat : http://rhn.redhat.com/errata/RHSA-2003-086.html
- Bulletin de sécurité DSA-260-1 de Debian : http://www.debian.org/security/
- Bulletin de sécurité NetBSD-SA2003-003 de NetBSD : ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-003.txt.asc
- Bulletin de sécurité SuSE-SA:2003:017 de SuSE : http://www.suse.com/de/security/2003_017_file.html
- Référence CVE CAN-2003-00102 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-00102

Gestion détaillée du document

10 mars 2003 version initiale.

13 mars 2003 ajout référence au bulletin de sécurité de Debian.

21 mars 2003 ajout référence au bulletin de sécurité de NetBSD.

24 mars 2003 ajout référence au bulletin de sécurité de SuSE. Ajout référence CVE.