Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 mars 2004
N° CERTA-2004-AVI-058

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des mtools sous Unix

Gestion du document

Référence	CERTA-2004-AVI-058
Titre	Vulnérabilité des mtools sous Unix
Date de la première version	01 mars 2004
Date de la dernière version	–
Source(s)	Avis de sécurité Mandrake Linux
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

- Atteintes à l'intégrité et à la confidentialité des données ;
- usurpation locale des privilèges administrateur.

2 Systèmes affectés

Tout système Unix avec la commande *mformat* des *mtools* installée avec les droits "set user id" (setuid) *root*.

3 Résumé

Un utilisateur local mal intentionné peut détourner la commande *mformat* pour lire ou écrire des fichiers arbitraires sur le système.

4 Description

Les *mtools* permettent d'accéder à des disques MS-DOS sans nécessité de monter les disques en question dans le système de fichiers. Afin de permettre à un utilisateur non privilégié d'utiliser ces commandes, ces outils peuvent être installés avec délégation des privilèges administrateur (setuid *root*).

mformat conservant ses privilèges, il est possible de détourner son fonctionnement pour accéder au système de fichiers avec les droits *root*.

5 Contournement provisoire

Supprimer les privilèges “setuid” *root* de la commande *mformat*.

6 Solution

Mettre à jour en suivant les recommendations de l'éditeur :

– Linux Mandrake :
http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:016

7 Documentation

Site des mtools :
http://mtools.linux.lu/

Gestion détaillée du document

01 mars 2004 version initiale.