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 août 2002
N° CERTA-2002-AVI-165

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnerabilité de la bibliothèque libmm

Gestion du document

Référence	CERTA-2002-AVI-165
Titre	Vulnerabilité de la bibliothèque libmm
Date de la première version	01 août 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité DSA 137-1 de Debian
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 ;
- modification de données.

2 Systèmes affectés

Toutes les versions de `libmm` jusqu'à la version 1.1.3 incluse.

3 Résumé

Une mauvaise gestion des accès concurrents à des fichiers temporaires permet à un utilisateur mal intentionné d'obtenir les privilèges de l'utilisateur privilégié `root`.

4 Description

La bibliothèque `libmm` (paquetage `mm`) fournit une interface de haut niveau permettant la communication inter-processus. Cette bibliothèque est utilisée par le serveur HTTP `apache`.

Une mauvaise gestion des accès concurrents à des fichiers temporaires permet à un utilisateur mal intentionné de forcer une application utilisant `libmm` à écrire dans un fichier arbitraire.

Cette vulnérabilité n'est exploitable que par un utilisateur local.

5 Solution

Appliquer les correctifs des différents éditeurs (Consultez la section documentation).

6 Documentation

- Avis de sécurité RHSA-2002:153 de RedHat :
  http://rhn.redhat.com/errata/RHSA-2002-153.html
- Avis de sécurité MDKSA-2002:045 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-045.php
- Avis de sécurité DSA 137-1 de Debian :
  http://www.debian.org/security
- Avis de sécurité SuSE-SA:2002:028 de SuSE :
  http://www.suse.de/de/security/

Gestion détaillée du document

01 août 2002 version initiale.