Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 mars 2003
N° CERTA-2003-AVI-037

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordements de mémoire dans de multiples fonctions de `libmcrypt` sous Linux

Gestion du document

Référence	CERTA-2003-AVI-037
Titre	Débordements de mémoire dans de multiples fonctions de `libmcrypt` sous Linux
Date de la première version	07 mars 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité DSA-228-1 de Debian bulletin de sécurité SuSE:2003:0010 de SuSE
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

- Augmentation de privilèges en local ;
- déni de service à distance.

2 Systèmes affectés

D'une façon générale, tous les systèmes utilisant une version de `libmcrypt` antérieure à 2.5.5 sont affectés.

- SuSE 7.1, 7.2, 7.3, 8.0, 8.1 ;
- SuSE eMail Server 3.1, III ;
- SuSE Linux Connectivity Server ;
- SuSE Linux Enterprise Server 7, 8 ;
- SuSE Linux Office Server ;
- Debian Linux (Woody et Sid), la version stable Potato ne mettait pas ce paquetage à disposition ;
- Gentoo Linux.

3 Résumé

Des débordements de mémoires dans plusieurs fonctions de `libmcrypt` permettent à un utilisateur local mal intentionné d'augmenter ses privilèges.

Des fuites de mémoires de `libmcrypt` permettent de saturer la mémoire dans des applications exécutées à distance.

4 Description

`libmcrypt` est un ensemble de fonctions utilisées pour le chiffrement de données. Cette librairie est utilisée seulement dans quelques applications (notamment par les développeurs de scripts PHP).

De multiples débordements de mémoires dans plusieurs fonctions de `libmcrypt` permettent à un utilisateur local d'augmenter ses privilèges.

D'autre part, la façon dont `libmcrypt` charge les algorithmes (via la librairie `libtool` ou `libtld` selon le système) dans les applications permanentes (serveurs web par exemple, ...), conduit à de petites fuites de mémoire (libération incomplète de la mémoire après chaque utilisation) qui peuvent aboutir à une saturation de la mémoire.

5 Contournement provisoire

Pour les système SuSE : se référer au bulletin de sécurité SuSE-SA:2003:0010 afin de connaître la démarche à suivre pour contourner les fuites de mémoire.

6 Solution

Consulter les bulletins de sécurité concernant les systèmes affectés pour connaître la disponibilité des correctifs.
La version 2.5.5 de `libmcrypt` corrige ces vulnérabilités.
Elle est disponible à l'adresse suivante :
ftp://mcrypt.hellug.gr/pub/mcrypt/libmcrypt

7 Documentation

- Le site web de `mcrypt` :
  http://mcrypt.hellug.gr/
- La liste des mises à jour de `libmcrypt` :
  http://cvs.hellug.gr/cgi-bin/viewcvs.cgi/mcrypt/libmcrypt/NEWS?rev=HEAD
- Bulletin de sécurité SuSE-SA:2003:0010 de SuSE :
  http://www.suse.com/de/security/2003_010_libmcrypt.html
- Bulletin de sécurité DSA-228-1 de Debian :
  http://www.debian.org/security/2003/dsa-228

Gestion détaillée du document

07 mars 2003 version initiale.