Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 janvier 2003
N° CERTA-2002-AVI-272-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de MySQL

Gestion du document

Référence	CERTA-2002-AVI-272-002
Titre	Multiples vulnérabilités de MySQL
Date de la première version	19 décembre 2002
Date de la dernière version	16 janvier 2003
Source(s)	Bulletin de sécurité "Multiple MySQL Vulnerabilities" d'e-matters
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 ;
- exécution de code arbitraire à distance ;
- déni de service.

2 Systèmes affectés

Versions de MySQL antérieures à la version 3.23.54.

3 Résumé

De multiples vulnérabilités ont été découvertes dans la base de données MySQL. Elles permettent à un utilisateur possédant un compte MySQL de réaliser un déni de service ou une élévation de privilèges.
Certaines de ces vulnérabilités sont exploitables sur des applications "client" utilisant la bibliothèque `libmysqlclient`.

4 Description

Deux vulnérabilités présentes dans le serveur de base de données MySQL permettent à un utilisateur légitime (possédant un compte MySQL) de provoquer un déni de service par arrêt brutal de l'application.

Une de ces vulnérabilités permet, sous certaines conditions, à un utilisateur mal intentionné d'exécuter du code arbitraire dans le contexte du serveur et réaliser ainsi une élévation de privilèges.

Deux vulnérabilités de type débordement de mémoire présentes dans les routines `read_rows` et `read_one_row` de la bibliothèque `libmysqlclient` peuvent être exploités par un utilisateur mal intentionné (par le biais d'un serveur MySQL compromis) pour exécuter du code arbitraire sur les clients.

L'exécution de code se fait dans le contexte de l'utilisateur qui lance l'application exploitant une version vulnérable de cette bibliothèque.

5 Solution

La version 3.23.54 de MySQL corrige ces vulnérabilités.

6 Documentation

- Bulletin de sécurité "Multiple MySQL Vulnerabilities" d'e-matters :
  http://security.e-matters.de/advisories/042002.html
- Nouveautés de la version 3.23.54 sur le site MySQL :
  http://www.mysql.com/doc/en/News-3.23.54.html
- Bulletin de sécurité DSA-212 de Debian :
  http://www.debian.org/security/2002/dsa-212
- Bulletin de sécurité MDKSA-2002:087 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2002:087
- Bulletin de sécurité SuSE-SA:2003:03 de SuSE :
  http://www.suse.com/de/security/2003_003_mysql.html
- Bulletin de sécurité RHSA-2002:288 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2002-288.html

Gestion détaillée du document

19 décembre 2002 version initiale.
06 janvier 2003 ajout référence au bulletin de sécurité SuSE-SA:2003:03 de SuSE.
16 janvier 2003 ajout référence au bulletin de sécurité RHSA-2002:288 de Red Hat.