



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 20 décembre 2004  
N° CERTA-2004-AVI-347-004

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans MySQL

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-347>

---

### Gestion du document

Référence	CERTA-2004-AVI-347-004
Titre	Vulnérabilités dans MySQL
Date de la première version	15 octobre 2004
Date de la dernière version	20 décembre 2004
Source(s)	Bulletins de sécurité Mysql
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

- Déni de service ;
- élévation de privilèges ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- MySQL 3.x ;
- MySQL 4.x.

## 3 Résumé

Deux vulnérabilités présentes sur le gestionnaire de base de données MySQL permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'élever ses privilèges sur le gestionnaire de base de données vulnérable.

## 4 Description

- Une vulnérabilité dans les requêtes SQL (Standard Query Language) de type « ALTER TABLE . . . RENAME » permet à un utilisateur mal intentionné d'élever ses privilèges et d'accéder à des informations confidentielles.
- Une seconde vulnérabilité permet à un utilisateur mal intentionné de réaliser un déni de service, via l'envoi de plusieurs requêtes SQL de type « ALTER ».

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les versions 3.23.59 et 4.0.21 corrigent ces vulnérabilités.

## 6 Documentation

- Site internet de Mysql :  
<http://www.mysql.com>
- Bulletin de sécurité de Mysql n°2408 :  
<http://bugs.mysql.com/bug.php?id=2408>
- Bulletin de sécurité de Mysql n°3270 :  
<http://bugs.mysql.com/bug.php?id=3270>
- Bulletin de sécurité Debian DSA-562 du 11 octobre 2004 :  
<http://www.debian.org/security/2004/dsa-562>
- Bulletin de sécurité RedHat RHSA-2004:569 du 20 octobre 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-569.html>
- Bulletin de sécurité RedHat RHSA-2004:597 du 20 octobre 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-597.html>
- Bulletin de sécurité RedHat RHSA-2004:611 du 27 octobre 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-611.html>
- Bulletin de sécurité Gentoo GLSA 200410-22 du 24 octobre 2004 :  
<http://www.gentoo.org/security/en/GLSA/GLSA-200410-22.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:119 du 01 novembre 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:119>
- Bulletin de sécurité SUSE SUSE-SR:2004:001 du 24 novembre 2004 :  
[http://www.suse.de/de/security/2004\\_01\\_sr.html](http://www.suse.de/de/security/2004_01_sr.html)
- Bulletins de sécurité FreeBSD du 16 décembre 2004 :  
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2004-0835 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0835>
- Référence CVE CAN-2004-0836 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0836>
- Référence CVE CAN-2004-0837 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0837>

## Gestion détaillée du document

**15 octobre 2004** version initiale.

**22 octobre 2004** ajout du bulletin de sécurité redhat.

**5 novembre 2004** ajout des références aux bulletins de sécurité Mandrake et Gentoo.

**25 novembre 2004** ajout des références aux bulletins de sécurité SUSE, Debian, RedHat et ajout de la référence CVE CAN-2004-0836.

**20 décembre 2004** ajout de la référence aux bulletins de sécurité FreeBSD du 16 décembre 2004.