Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mars 2008
N° CERTA-2008-AVI-162

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans MySQL

Gestion du document

Référence	CERTA-2008-AVI-162
Titre	Vulnérabilités dans MySQL
Date de la première version	27 mars 2008
Date de la dernière version	–
Source(s)	
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

- Exécution de code arbitraire à distance ;
- déni de service à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

MySQL, version 4.1.23 et antérieures.

3 Résumé

Plusieurs vulnérabilités affectent les versions 4.x du gestionnaire de base de données *MySQL*. En particulier, certaines d'entre elles permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

De nombreuses vulnérabilités affectent la branche 4 de *MySQL*.

La création de tables *MyISAM* avec certaines options permet d'écraser des tables existantes.

Le renommage utilisé avec certains paramètres permet la réécriture de tables système.

Des erreurs provoquent des débordements de mémoire ou de pile ou des violations de la segmentation de la mémoire. Dans certains cas l'exploitation permet à un utilisateur d'exécuter du code arbitraire à distance.

Certaines erreurs permettent de provoquer un arrêt inopiné (*crash*) du serveur. L'utilisation d'un paquet d'authentification malformé permet de provoquer cet arrêt à distance.

Certaines erreurs conduisent à des insertions dans les affichages ou à la corruption de tables.

5 Solution

La version 4.1.24 corrige ces problèmes. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

Note : la branche 4 du logiciel MySQL n'est plus maintenue (cf. section Documentation). Il est recommandé de migrer vers la branche 5 de ce logiciel.

6 Documentation

- Bulletin de version de MySQL :
  http://dev.mysql.com/doc/refman/4.1/en/news-4-1-24.html
- Politique et calendrier de support pour MySQL :
  http://www.mysql.com/company/legal/lifecycle/
- Référence CVE CVE-2007-3780 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3780
- Référence CVE CVE-2007-5969 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5969

Gestion détaillée du document

27 mars 2008 version initiale.