Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 août 2006
N° CERTA-2006-AVI-350-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Mysql

Gestion du document

Référence	CERTA-2006-AVI-350-001
Titre	Vulnérabilités dans Mysql
Date de la première version	09 août 2006
Date de la dernière version	21 août 2006
Source(s)	Bulletin 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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Mysql 3.x ;
- Mysql 4.x antérieures à la version 4.1.21 ;
- Mysql 5.x antérieures à la version 5.0.24.

3 Résumé

Plusieurs vulnérabilité présentes dans MySQL peuvent être exploitées par un utilisateur mal intentionné pour porter atteinte à l'intégrité et à la confidentialité des données ou encore pour élever ses privilèges dans le gestionnaire de base de données.

4 Description

Trois vulnérabilités dans le traitement de certaines fonctions sont présentes dans MySQL :

- Une vulnérabilité est présente dans le traitement de la fonction `STR_TO_DATE`. Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné, via une requête malveillante contenant la clause `STR_TO_DATE`, pour réaliser un déni de service du gestionnaire de base de données (CVE-2006-3081) ;
- une seconde vulnérabilité présente dans le traitement de la clause `DATE_FORMAT` peut être exploitée pour réaliser un déni de service (CVE-2006-3469) ;
- une troisième vulnérabilité est présente dans la fonction `mysql_real_escape_string`. Un utilisateur mal intentionné peut, via une requête SQL malveillante, réaliser une attaque par injection SQLi (CVE-2006-2753).

Une autre vulnérabilité est présente sur la fonction `MERGE`. Cette vulnérabilité permet à un utilisateur d'élever ses privilèges sur le système.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité MySQL 4.x :
  http://dev.mysql.com/doc/refman/4.1/en/news-4-1-21.html
- Bulletin de sécurité MySQL 5.x :
  http://dev.mysql.com/doc/refman/4.1/en/news-5-0-24.html
- Bulletin de sécurité Debian :
  http://www.vuxml.org/freebsd/pkg-mysql-server.html
- Référence CVE CVE-2006-2753 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2753
- Référence CVE CVE-2006-3081 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3081
- Référence CVE CVE-2006-3469 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3469

Gestion détaillée du document

09 août 2006 version initiale.
21 août 2006 ajout de la référence au bulletin de sécurité FreeBSD.