



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 mars 2005
N° CERTA-2005-AVI-110-002

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-2005-AVI-110>

Gestion du document

Référence	CERTA-2005-AVI-110-002
Titre	Vulnérabilités dans Mysql
Date de la première version	14 mars 2005
Date de la dernière version	29 mars 2005
Source(s)	Avis 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

- Elévation de privilèges ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

MySQL versions 4.x antérieures à la version 4.0.24.

3 Résumé

Deux vulnérabilités présentes dans MySQL peuvent être exploitées par un utilisateur local mal intentionné pour accéder au système ou élever ses privilèges sur le système vulnérable.

4 Description

Deux vulnérabilités sont présentes sur MySQL :

- Une vulnérabilité présente dans la fonction `udf_init()` permet à un utilisateur mal intentionné, via l'utilisation des commandes `INSERT INTO` ou `CREATE FUNCTION` de charger une librairie. Cette vulnérabi-

lité ne peut être exploitée que si le serveur MySQL a été compilé avec les options permettant aux utilisateurs de charger des fonctions udf (User Defined Function).

- La seconde vulnérabilité concerne une mauvaise gestion des fichiers temporaires lors de l'utilisation de la fonction `CREATE TEMPORARY TABLE`. Un utilisateur mal intentionné peut exploiter cette vulnérabilité via l'utilisation d'un lien symbolique pour écraser des fichiers arbitraires sur le système.

5 Solution

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

6 Documentation

- Site internet de MySQL :
<http://www.mysql.com>
- Bulletin de sécurité MySQL :
http://www.mysql.com/news-and-events/news/article_883.html
- Bulletin de sécurité Gentoo GLSA 200503-19 du 16 mars 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200503-19.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:060 du 21 mars 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:060>
- Bulletin de sécurité RedHat RHSA-2005:334-07 du 28 mars 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-334.html>
- Bulletin de sécurité SUSE-SA:2005:019 du 24 mars 2005 :
http://www.novell.com/linux/security/advisories/2005_19_mysql.html
- Bulletin de sécurité FreeBSD pour mysql-server du 14 mars 2005 :
<http://www.vuxml.org/freebsd/pkg-mysql-server.html>
- Référence CVE CAN-2005-0709 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0709>
- Référence CVE CAN-2005-0710 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0710>
- Référence CVE CAN-2005-0711 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0711>

Gestion détaillée du document

14 mars 2005 version initiale.

25 mars 2005 ajout référence aux bulletins de sécurité Gentoo, Mandrake, SuSE et FreeBSD.

29 mars 2005 ajout référence au bulletin de sécurité RedHat et aux références CVE.