

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-2007-AVI-222>

Gestion du document

Référence	CERTA-2007-AVI-222
Titre	Vulnérabilités dans MySQL
Date de la première version	18 mai 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité MySQL du 21 et 29 mars 2007
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- MySQL version 4.1 ;
- MySQL version 5.0 ;
- MySQL version 5.0.40 ;
- MySQL version 5.1.

3 Résumé

Deux vulnérabilités de MySQL permettent à un utilisateur de contourner la politique de sécurité et d'élever ses privilèges.

4 Description

Deux vulnérabilités sont présentes dans MySQL :

- la première (27515), permet à un utilisateur connecté à la base de renommer dans certaines conditions une table sans posséder le privilège DROP ;
- la seconde (27337), permet à un utilisateur d'élever ses privilèges en utilisant des procédures stockées de façon particulière.

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 27337 du 29 mars 2007 :
<http://bugs.mysql.com/bug.php?id=27337>
- Bulletin de sécurité MySQL 27515 du 29 mars 2007 :
<http://bugs.mysql.com/bug.php?id=27515>
- Référence CVE CVE-2007-2691 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2691>
- Référence CVE CVE-2007-2692 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2692>

Gestion détaillée du document

18 mai 2007 version initiale.