

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-223>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2004-AVI-223 |
| Titre | Vulnérabilité de MySQL |
| Date de la première version | 06 juillet 2004 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité NGS Research du 01 juillet 2004 |
| 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 du mécanisme d'authentification ;
- exécution de code arbitraire possible.

2 Systèmes affectés

- Toutes les versions de MySQL de la branche 4.1 antérieures à la version 4.1.3 ;
- MySQL 5.0.

3 Résumé

Deux vulnérabilités de MySQL permettent à un utilisateur mal intentionné de contourner le mécanisme d'authentification.

4 Description

MySQL est un serveur de base de données open source.

Une première vulnérabilité permet à un utilisateur mal intentionné de contourner le mécanisme d'authentification

par mot de passe.

Une seconde vulnérabilité permet à un utilisateur mal intentionné de déclencher un débordement de mémoire dans le mécanisme d'authentification.

5 Solution

- La version de MySQL 4.1.3 corrige ces vulnérabilités ;
- la version de MySQL 5.0 corrigera ces vulnérabilités.

MySQL est téléchargeable à l'adresse suivante :

<http://www.mysql.com/downloads/>

6 Documentation

- Site Internet de MySQL :
<http://www.mysql.com>
- Bulletin de sécurité NGS Research du 01 juillet 2004 :
<http://www.nextgenss.com/advisories/mysql-authbypass.txt>

Gestion détaillée du document

06 juillet 2004 version initiale.