

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-2010-AVI-399>

Gestion du document

Référence	CERTA-2010-AVI-399-001
Titre	Vulnérabilités dans MySQL
Date de la première version	24 août 2010
Date de la dernière version	26 août 2010
Source(s)	Bulletins de version 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

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

2 Systèmes affectés

- MySQL version 5.1.48 et versions antérieures ;
- MySQL version 5.5.4 et versions antérieures ;

3 Résumé

De nombreuses vulnérabilités présentes dans MySQL ont été corrigées. Les plus importantes permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent MySQL :

- une erreur de la vérification des droits d'accès permet à un utilisateur malveillant de désinstaller un greffon à distance ;
- une erreur de vérification de droits d'accès permet à un utilisateur malveillant authentifié disposant de certains droits sur une table de lire ou de modifier les autres tables présentes sur le serveur ;
- une déficience dans la gestion des paquets réseau permet à un utilisateur malveillant d'épuiser les ressources du serveur à distance ;
- un défaut de vérification des bornes dans un argument qui est un nom de table permet à un utilisateur malveillant authentifié d'exécuter du code arbitraire à distance ;
- un utilisateur malveillant authentifié disposant de certains privilèges peut provoquer un déni de service ou déplacer des répertoires de données à distance.

5 Solution

Les versions 5.1.49, 5.1.50 et 5.5.5 de MySQL remédient à ces problèmes. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de la version 5.1.49 de MySQL du 09 juillet 2010 :
<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html>
- Bulletin de la version 5.1.50 de MySQL du 03 août 2010 :
<http://dev.mysql.com/doc/refman/5.1/en/news-5-1-50.html>
- Bulletin de la version 5.5.5 de MySQL du 06 juillet 2010 :
<http://dev.mysql.com/doc/refman/5.5/en/news-5-5-5.html>
- Référence CVE CVE-2010-1621 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1621>
- Référence CVE CVE-2010-1848 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1848>
- Référence CVE CVE-2010-1849 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1849>
- Référence CVE CVE-2010-1850 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1850>
- Référence CVE CVE-2010-2008 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2008>

Gestion détaillée du document

24 août 2010 version initiale.

26 août 2010 rectification des liens vers les bulletins de l'éditeur.