

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2006-AVI-137>

Gestion du document

Référence	CERTA-2006-AVI-137-001
Titre	Vulnérabilité dans MySQL
Date de la première version	05 avril 2006
Date de la dernière version	24 mai 2006
Source(s)	
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.

2 Systèmes affectés

Package *MySQL* dans les versions :

- Corporate 3.0
- 2006.0
- 10.2

3 Description

Cette vulnérabilité dans *MySQL* permet à un utilisateur de contourner la politique de sécurité en trompant le mécanisme de journalisation via une requête SQL contenant le caractère NULL. Ce caractère n'est ensuite pas correctement interprété par la fonction `mysql_real_query`.

4 Solution

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

5 Documentation

- Bulletin de sécurité Mandriva MDKSA-2006:064 du 05 avril 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:064>
- Bulletin de sécurité Debian DSA-1071 du 22 mai 2006 :
<http://www.debian.org/security/2006/dsa-1071>
- Bulletin de sécurité Debian DSA-1073 du 22 mai 2006 :
<http://www.debian.org/security/2006/dsa-1073>
- Référence CVE CAN-2006-0903 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0903>
- Site de rapport d'incidents MySQL :
<http://bugs.mysql.com/bug.php?id=17667>

Gestion détaillée du document

05 avril 2006 version initiale ;

24 mai 2006 ajout des références aux Bulletins de sécurité Debian.