

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-2005-AVI-079>

Gestion du document

Référence	CERTA-2005-AVI-079-001
Titre	Vulnérabilité de MySQL
Date de la première version	15 février 2005
Date de la dernière version	18 février 2005
Source(s)	Bulletin de sécurité Mandrake MDKSA-2005:036
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

Atteinte à l'intégrité des données.

2 Systèmes affectés

Serveur de bases de données *MySQL*.

3 Résumé

Une vulnérabilité dans le serveur de bases de données *MySQL* permet à un utilisateur mal intentionné d'écraser des fichiers arbitraires.

4 Description

Le script *mysqlaccess* du serveur de bases de données *MySQL* crée des fichiers temporaires avec des noms prévisibles.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité via des liens symboliques pour écraser un fichier arbitraire du 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 Debian DSA-647 du 19 janvier 2005 :
<http://www.debian.org/security/2005/dsa-647>
- Bulletin de sécurité Gentoo GLSA 200501-33 du 23 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-33.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:036 du 10 février 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:036>
- Bulletin de sécurité FreeBSD pour mysql-scripts du 16 janvier 2005 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité OpenBSD pour mysql-server du 19 janvier 2005 :
<http://www.vuxml.org/openbsd/>
- Référence CVE CAN-2005-0004 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0004>

Gestion détaillée du document

15 février 2005 version initiale.

18 février 2005 ajout du site Internet de MySQL et de la référence CVE CAN-2005-0004 et correction des liens FreeBSD et OpenBSD.