

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur de base de données 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-2003-AVI-151>

Gestion du document

Référence	CERTA-2003-AVI-151-002
Titre	Vulnérabilité du serveur de base de données MySQL
Date de la première version	16 septembre 2003
Date de la dernière version	10 octobre 2003
Source(s)	Bulletin de sécurité DSA-381 de Debian Bulletin de sécurité 200309-08 de Gentoo
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

Elévation de privilèges.

2 Systèmes affectés

- MySQL versions 3.23.57 et antérieures ;
- MySQL versions 4.0.14 et antérieures.

3 Description

Une vulnérabilité est présente dans une routine de contrôle des mots de passe.

Un utilisateur légitime de MySQL possédant le droit d'administration ALTER sur la table `mysql.user` peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire sur la plate-forme hébergeant le serveur MySQL avec les privilèges du processus `mysqld`.

4 Solution

Les versions 3.23.58 et 4.0.15 de MySQL corrigent cette vulnérabilité :

- Annonce MySQL 4.0.15 :
<http://lists.mysql.com/announce/168>
- Annonce MySQL 3.23.58 :
<http://www.mysql.com/doc/en/News-3.23.58.html>

5 Documentation

- Bulletin de sécurité DSA-381 de Debian :
<http://www.debian.org/security/2003/dsa-381>
- Bulletin de sécurité 200309-08 de Gentoo :
<http://www.securityfocus.com/advisories/5812>
- Bulletin de sécurité SuSE-SA:2003:042 de SuSE :
http://www.suse.com/de/security/2003_042_mysql.html
- Bulletin de sécurité MDKSA-2003:094 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:094>
- Bulletin de sécurité RHSA-2003:281 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-281.html>
- Bulletin de sécurité RHSA-2003:282 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-282.html>
- Référence CVE CAN-2003-0780 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0780>

Gestion détaillée du document

16 septembre 2003 version initiale.

02 octobre 2003 ajout références aux bulletins de SuSE et Mandrake.

10 octobre 2003 ajout références aux bulletins de Red Hat.