Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 22 octobre 2004
N° CERTA-2004-AVI-283-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans MySQL

Gestion du document

Référence	CERTA-2004-AVI-283-003
Titre	Vulnérabilité dans MySQL
Date de la première version	31 août 2004
Date de la dernière version	22 octobre 2004
Source(s)	Bulletin de sécurité DSA-540 de Debian
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

MySQL versions 4.0.20 et antérieures.

3 Résumé

Une vulnérabilité a été découverte dans MySQL permettant à un individu mal intentionné de réécrire sur des fichiers existants ou d'en créer de nouveaux sur le système affecté.

4 Description

`mysqlhotcopy` est un script écrit en PERL utilisant la commande `cp` ou `scp` afin d'effectuer des sauvegardes de tables ou de bases MySQL.

Il utilise des fichiers temporaires dont les noms sont prédictibles. Cette vulnérabilité peut être exploitée par un utilisateur local mal intentionné afin de corrompre n'importe quel fichier du système.

5 Solution

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

6 Documentation

- Bulletin de sécurité DSA-540 de Debian du 18 août 2004 :
  http://www.debian.org/security/2004/dsa-540
- Bulletin de sécurité RedHat du 20 octobre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-597.html
- Bulletin de sécurité RedHat du 20 octobre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-569.html
- Bulletin de sécurité Gentoo GLSA 200409-02 du 01 septembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200409-02.xml
- Bulletin de sécurité OpenBSD pour mysql-server du 20 août 2004 :
  http://www.vuxml.org/openbsd/
- Référence CVE CAN-2004-0457 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0457

Gestion détaillée du document

31 août 2004 version initiale.
01 septembre 2004 ajout de la référence au bulletin de sécurité OpenBSD.
02 septembre 2004 ajout de la référence au bulletin de sécurité Gentoo.
22 octobre 2004 ajout de la référence au bulletin de sécurité RedHat.