Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juin 2006
N° CERTA-2006-AVI-182-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mutliples vulnérabilités sur MySQL

Gestion du document

Référence	CERTA-2006-AVI-182-004
Titre	Mutliples vulnérabilités sur MySQL
Date de la première version	04 mai 2006
Date de la dernière version	28 juin 2006
Source(s)	Bulletins de sécurité 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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- MySQL 4.x ;
- MySQL 5.x.

3 Résumé

Plusieurs vulnérabilités sont présentes dans MySQL. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné pour porter atteinte à l'intégrité des données ou exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités sont présentes dans le code traitant les paquets malformés `COM_TABLE_DUMP` peuvent être utilisée par un utilisateur déjà authentifié pour porter atteinte à l'intégrité des données ou pour exécuter du code arbitraire.

Une vulnérabilité dans le traitement des identifications invalides peut être exploitée par un utilisateur mal intentionné pour porter atteinte à la confidentialité des données.

5 Solution

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

6 Documentation

- Bulletin de sécurité MySQL 4-1-19 :
  http://dev.mysql.com/doc/refman/4.1/en/news-4-1-19.html
- Bulletin de sécurité MySQL 5-0-21 :
  http://dev.mysql.com/doc/connector/j/en/news-5-0-21.html
- Bulletin de sécurité MySQL 5-1-10 :
  http://dev.mysql.com/doc/refman/5.1/en/news-5-1-10.html
- Bulletin de sécurité Gentoo GLSA 200605-13 du 15 mai 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200605-13.xml
- Bulletin de sécurité Mandriva MDKSA-2006:084 du 16 mai 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:084
- 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
- Bulletin de sécurité Debian DSA-1079 du 29 mai 2006 :
  http://www.debian.org/security/2006/dsa-1079
- Bulletin de sécurité SUSE SUSE-SR:2006:012 du 02 juin 2006 :
  http://www.novell.com/linux/security/advisories/2006-06-02.html
- Bulletin de sécurité SUSE SUSE-SA:2006:036 du 23 juin 2006 :
  http://www.novell.com/linux/security/advisories/2006_36_mysql.html
- Référence CVE CVE-2006-1516 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1516
- Référence CVE CVE-2006-1517 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1517
- Référence CVE CVE-2006-1518 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1518

Gestion détaillée du document

04 mai 2006 version initiale ;
16 mai 2006 ajout des références CVE et de la référence au bulletin de sécurité Mandriva ;
24 mai 2006 ajout des références aux bulletins de sécurité Debian.
08 juin 2006 ajout des références aux bulletins de sécurité Gentoo, Debian et SUSE.
28 juin 2006 ajout de la référence au bulletin de sécurité SUSE.