Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 mai 2010
N° CERTA-2010-AVI-223

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans MySQL

Gestion du document

Référence	CERTA-2010-AVI-223
Titre	Multiples vulnérabilités dans MySQL
Date de la première version	21 mai 2010
Date de la dernière version	–
Source(s)	Note de nouvelle version MySQL 5.1.47 du 06 mai 2010
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 à distance ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

MySQL 5.1.x versions antérieures à la 5.1.47.

3 Résumé

Plusieurs vulnérabilités dans `MySQL` permettent à une personne malintentionnée de contourner la politique de sécurité, de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités dans `MySQL` ont été découvertes :

- une erreur dans la gestion des paramètres de la commande *COM_FIELD_LIST* permet de contourner la politique de sécurité (CVE-2010-1848) ;

– une erreur non spécifiée par l'éditeur dans la gestion de la taille de certains paquets permet de provoquer un déni de service à distance (CVE-2010-1849) ;
– une vulnérabilité de type dépassement de la mémoire tampon dans la gestion du paramètre de nom de table de la commande *COM_FIELD_LIST* permet d'exécuter du code arbitraire à distance (CVE-2010-1850).

5 Solution

Se référer à la note de nouvelle version de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Note de nouvelle version MySQL 5.1.47 du 06 mai 2010 :
http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html
– Référence CVE CVE-2010-1848 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1848
– Référence CVE CVE-2010-1849 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1849
– Référence CVE CVE-2010-1850 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1850

Gestion détaillée du document

21 mai 2010 version initiale.