Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 janvier 2013
N° CERTA-2012-ALE-007-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans MySQL

Gestion du document

Référence	CERTA-2012-ALE-007-001
Titre	Vulnérabilité dans MySQL
Date de la première version	06 décembre 2012
Date de la dernière version	07 janvier 2013
Source(s)	Bulletin de sécurité CVE-2012-5611 du 03 decembre 2012
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.

2 Systèmes affectés

Toutes les versions MySQL supportées par Oracle.

3 Résumé

Une vulnérabilité a été découverte dans *Oracle MySQL*. Elle permet une exécution de code arbitraire à distance au moyen d'une requête SQL spécialement conçue. Il est possible de provoquer un débordement de mémoire tampon dans la pile et de contrôler le flux d'exécution pour exécuter du code malveillant. L'attaque nécessite un compte sur le serveur *MySQL*. Les hébergeurs mutualisés de base de données sont donc particulièrement impactés.

4 Solution

Installer la dernière version stable de *Oracle MySQL* (>= version 5.5.29).

5 Documentation

- Référence CVE-2012-5611 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5611
- MySQL (Linux) Stack Based buffer overrun PoC Zeroday :
  http://seclists.org/fulldisclosure/2012/Dec/4
- Outil de réduction des risques liés aux exploitations EMET :
  http://www.microsoft.com/en-us/download/details.aspx?id=29851

Gestion détaillée du document

06 décembre 2012 version initiale.
07 janvier 2013 fermeture de l'alerte, suite à la correction silencieuse par l'éditeur.