Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 octobre 2009
N° CERTA-2009-AVI-447

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans phpMyAdmin

Gestion du document

Référence	CERTA-2009-AVI-447
Titre	Vulnérabilités dans phpMyAdmin
Date de la première version	16 octobre 2009
Date de la dernière version	–
Source(s)	Annonce de sécurité phpMyAdmin PMASA-2009-6 du 13 octobre 2009
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

- Injection de code indirecte ;
- exécution de requêtes SQL arbitraires.

2 Systèmes affectés

- phpMyAdmin 2.11.x ;
- phpMyAdmin 3.x.

3 Résumé

Deux vulnérabilités découvertes dans `phpMyAdmin` permettent à un utilisateur distant malintentionné d'exécuter des requêtes `SQL` (*Structured Query Language*) ou de réaliser une injection de code indirecte.

4 Description

Une vulnérabilité dans le traitement des noms de tables `MySQL` peut être exploitée afin d'injecter du code arbitraire qui sera exécuté dans le contexte du navigateur Internet d'un utilisateur.

Une autre vulnérabilité, causée par une erreur dans le traitement des entrées fournies à la fonctionnalité `PDF schema generator`, peut être exploitée afin d'exécuter des requêtes `SQL` arbitraires.

5 Solution

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

6 Documentation

- Annonce de sécurité phpMyAdmin PMASA-2009-6 du 13 octobre 2009 :
  http://www.phpmyadmin.net/home_page/security/PMASA-2009-6.php
- Référence CVE CVE-2009-3696 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3696
- Référence CVE CVE-2009-3697 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3697

Gestion détaillée du document

16 octobre 2009 version initiale.