

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans phpMyAdmin

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-422>

Gestion du document

Référence	CERTA-2005-AVI-422
Titre	Vulnérabilité dans phpMyAdmin
Date de la première version	25 octobre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité phpMyAdmin PMASA-2005-5 du 22 octobre 2005
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 la confidentialité des données ;
- attaque de type *Cross-Site Scripting*.

2 Systèmes affectés

phpMyAdmin versions 2.6.4-pl2 et antérieures.

3 Résumé

Deux vulnérabilités présentes dans phpMyAdmin permettent à un utilisateur distant de porter atteinte à la confidentialité des données ou d'effectuer une attaque de type *Cross-Site Scripting*.

4 Description

Deux vulnérabilités sont présentes dans phpMyAdmin :

- La première vulnérabilité est due à un manque de contrôle des paramètres passés à certains scripts php permettant à un utilisateur mal intentionné de modifier certains paramètres sensibles de phpMyAdmin par le biais d'une requête malicieusement construite.

- la seconde vulnérabilité est due à une vérification trop faible des paramètres passés aux scripts : `left.php`, `queryframe.php` et `server_databases.php`. Ceci permet d'exécuter du script potentiellement malveillant au cours d'une consultation par un navigateur tierce.

Ces deux failles permettent soit de porter atteinte à la confidentialité des données soit d'effectuer une attaque de type *Cross-Site Scripting*.

5 Solution

La version 2.6.4-pl3 de phpMyAdmin corrige le problème :
http://www.phpmyadmin.net/home_page/downloads.php

6 Documentation

- Site de phpMyAdmin :
<http://www.phpmyadmin.net>
- Bulletin de sécurité phpMyAdmin PMASA-2005-5 du 22 octobre 2005 :
http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2005-5

Gestion détaillée du document

25 octobre 2005 version initiale.