

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2010-AVI-397>

Gestion du document

Référence	CERTA-2010-AVI-397
Titre	Vulnérabilités dans phpMyAdmin
Date de la première version	23 août 2010
Date de la dernière version	–
Source(s)	Notes de sécurité phpMyAdmin du 20 août 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 ;
- injection de code indirecte à distance.

2 Systèmes affectés

- Branche 2.x de *phpMyAdmin* : versions inférieures à 2.11.10.1 ;
- branche 3.x de *phpMyAdmin* : versions inférieures à 3.3.5.1 .

3 Résumé

Des vulnérabilités dans *phpMyAdmin* permettent notamment à un attaquant d'inclure du code *PHP* dans un fichier de configuration.

4 Description

Plusieurs vulnérabilités ont été découvertes dans *phpMyAdmin* :

- une vulnérabilité (CVE-2010-3055) permet à une personne malveillante d'insérer du code *PHP* dans un fichier de configuration, via le script d'installation. L'exploitation de cette faille ne peut réussir que si les

- bonnes pratiques d'installation de *phpMyAdmin* n'ont pas été suivies, et que les scripts d'installation n'ont pas été supprimés une fois celle-ci terminée. Cette faille ne touche que les versions inférieures à 2.11.10.1 ;
- les versions inférieures à 3.3.5.1 pour la branche 3.x et inférieures à 2.11.10.1 pour la branche 2.x sont vulnérables à une attaque de type injection de code indirecte à distance sur de nombreuses pages (CVE-2010-3056).

5 Solution

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

6 Documentation

- Notes de sécurité *phpMyAdmin* du 20 août 2010 :
http://www.phpmyadmin.net/home_page/security/PMASA-2010-4.php
http://www.phpmyadmin.net/home_page/security/PMASA-2010-5.php
- Référence CVE CVE-2010-3055 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3055>
- Référence CVE CVE-2010-3056 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3056>

Gestion détaillée du document

23 août 2010 version initiale.