

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-2008-AVI-464>

Gestion du document

Référence	CERTA-2008-AVI-464-001
Titre	Vulnérabilité dans phpMyAdmin
Date de la première version	16 septembre 2008
Date de la dernière version	30 septembre 2008
Source(s)	Bulletin de sécurité phpMyAdmin PMASA-2008-7 du 15 septembre 2008
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

– phpMyAdmin 2.x.

3 Résumé

Une vulnérabilité dans phpMyAdmin permet à un utilisateur distant d'exécuter du code arbitraire.

4 Description

Une vulnérabilité dans le fichier `server_databases.php` permet à un utilisateur distant, précédemment authentifié, d'exécuter du code arbitraire de type `shell`.

Cette vulnérabilité ne peut être exploitée que si la configuration du serveur PHP autorise les commandes de type `exec`.

5 Solution

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

6 Documentation

- Bulletin de sécurité FEDORA-2008-8269
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01137.html>
- Bulletin de sécurité FEDORA-2008-8286
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01155.html>
- Bulletin de sécurité FEDORA-2008-8335
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01228.html>
- Bulletin de sécurité FEDORA-2008-8370
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01290.html>
- Bulletin de sécurité phpMyAdmin PMASA-2008-7 du 15 septembre 2008 :
http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2008-7
- Référence CVE CVE-2008-4096 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4096>

Gestion détaillée du document

16 septembre 2008 version initiale.

19 septembre 2008 ajout de la référence CVE.

30 septembre 2008 Ajout Fedora.