

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples 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-2011-AVI-380>

---

### Gestion du document

Référence	CERTA-2011-AVI-380
Titre	Multiples vulnérabilités dans phpMyAdmin
Date de la première version	05 juillet 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité phpMyAdmin du 03 juillet 2011
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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- phpMyAdmin versions 3.3.10.1 et antérieures ;
- phpMyAdmin versions 3.4.3.0 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités dans phpMyAdmin permettent à un utilisateur distant d'exécuter du code arbitraire, de porter atteinte à l'intégrité ou à la confidentialité de certaines données.

## 4 Description

Plusieurs vulnérabilités sont présentes dans `phpMyAdmin` :

- la première permet de modifier le contenu de certaines variables de session et ce faisant d'exécuter du code arbitraire ;
- la seconde concerne un manque de contrôle sur certaines URL passées au serveur et permet d'exécuter du code arbitraire à distance ;
- la troisième vulnérabilité relative à un manque de contrôle des expressions régulières permet de conduire des attaques de type traversée de répertoire ;
- la dernière concerne également un problème de traversée de répertoire lié à la gestion de certains types MIME.

## 5 Solution

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

## 6 Documentation

- Bulletins de sécurité `phpMyAdmin` PMASA-2011-5 du 02 juillet 2011 :  
[http://www.phpmyadmin.net/home\\_page/security/PMASA-2011-5.php](http://www.phpmyadmin.net/home_page/security/PMASA-2011-5.php)
- Bulletins de sécurité `phpMyAdmin` PMASA-2011-6 du 02 juillet 2011 :  
[http://www.phpmyadmin.net/home\\_page/security/PMASA-2011-6.php](http://www.phpmyadmin.net/home_page/security/PMASA-2011-6.php)
- Bulletins de sécurité `phpMyAdmin` PMASA-2011-7 du 02 juillet 2011 :  
[http://www.phpmyadmin.net/home\\_page/security/PMASA-2011-7.php](http://www.phpmyadmin.net/home_page/security/PMASA-2011-7.php)
- Bulletins de sécurité `phpMyAdmin` PMASA-2011-8 du 02 juillet 2011 :  
[http://www.phpmyadmin.net/home\\_page/security/PMASA-2011-8.php](http://www.phpmyadmin.net/home_page/security/PMASA-2011-8.php)
- Référence CVE CVE-2011-2505 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2505>
- Référence CVE CVE-2011-2506 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2506>
- Référence CVE CVE-2011-2507 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2507>
- Référence CVE CVE-2011-2508 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2508>

## Gestion détaillée du document

**05 juillet 2011** version initiale.