

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-2011-AVI-411>

---

### Gestion du document

Référence	CERTA-2011-AVI-411
Titre	Vulnérabilités dans phpMyAdmin
Date de la première version	26 juillet 2011
Date de la dernière version	–
Sources	Bulletins de sécurité phpMyAdmin PMASA-2011-9 à PMASA-2011-12 du 23 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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

phpMyAdmin 3.4.x et 3.3.x.

## 3 Résumé

Plusieurs vulnérabilités affectent phpMyAdmin. Certaines permettent d'exécuter à distance du code sur le serveur vulnérable.

## 4 Description

Quatre vulnérabilités de phpMyAdmin ont été corrigées :

- un défaut dans le script d'affichage des tables permet de réaliser de l'injection de code indirecte (XSS) ;

- dans certaines configurations, une transformation de type MIME permet de réaliser de l'injection de code locale (LFI) ;
- une vulnérabilité permet de réaliser de l'injection de code locale (LFI). Cette exploitation requiert une authentification préalable ;
- des variables PHP, parmi lesquels la variable *SESSION*, peuvent être manipulées.

## 5 Solution

Les versions 3.3.10.3 et 3.4.3.2 de phpMyAdmin corrigent ces problèmes.

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

## 6 Documentation

- Bulletins de sécurité phpMyAdmin PMASA-2011-9 à PMASA-2011-12 du 23 juillet 2011 :
  - [http://www.phpmyadmin.net/home\\_page/security/PMASA-2011-9.php](http://www.phpmyadmin.net/home_page/security/PMASA-2011-9.php)
  - [http://www.phpmyadmin.net/home\\_page/security/PMASA-2011-10.php](http://www.phpmyadmin.net/home_page/security/PMASA-2011-10.php)
  - [http://www.phpmyadmin.net/home\\_page/security/PMASA-2011-11.php](http://www.phpmyadmin.net/home_page/security/PMASA-2011-11.php)
  - [http://www.phpmyadmin.net/home\\_page/security/PMASA-2011-12.php](http://www.phpmyadmin.net/home_page/security/PMASA-2011-12.php)
- Référence CVE CVE-2011-2642 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2642>
- Référence CVE CVE-2011-2643 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2643>

## Gestion détaillée du document

**26 juillet 2011** version initiale.