

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-2009-AVI-117>

---

### Gestion du document

Référence	CERTA-2009-AVI-117
Titre	Vulnérabilités dans phpMyAdmin
Date de la première version	26 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité phpMyAdmin PMASA-2009-1 du 24 mars 2009 Bulletin de sécurité phpMyAdmin PMASA-2009-2 du 24 mars 2009 Bulletin de sécurité phpMyAdmin PMASA-2009-3 du 24 mars 2009
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 ;
- injections de code indirectes.

## 2 Systèmes affectés

- *phpMyAdmin* versions 2.11.x antérieures à 2.11.9.5 ;
- *phpMyAdmin* versions 3.x antérieures à 3.1.3.1.

## 3 Résumé

Plusieurs vulnérabilités dans *phpMyAdmin* permettent de réaliser des injections de code indirectes et d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans *phpMyAdmin* :

- la fonctionnalité des flux BLOB permet d’inclure des fichiers distants et d’injecter des entêtes HTTP (PMASA-2009-1). Cette vulnérabilité n’affecte que les versions depuis 3.1.0.0 ;
- la page d’export fait appel à des *cookies* qui peuvent être modifiés de telle sorte à réaliser une attaque de type *cross-site scripting* (PMASA-2009-2) ;
- les scripts d’installation utilisés pour créer le fichier de configuration peuvent être détournés au moyen d’une requête POST afin de provoquer l’inclusion d’un fichier distant (PMASA-2009-3).

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité phpMyAdmin PMASA-2009-1 du 24 mars 2009 :  
[http://www.phpmyadmin.net/home\\_page/security/PMASA-2009-1.php](http://www.phpmyadmin.net/home_page/security/PMASA-2009-1.php)
- Bulletin de sécurité phpMyAdmin PMASA-2009-2 du 24 mars 2009 :  
[http://www.phpmyadmin.net/home\\_page/security/PMASA-2009-2.php](http://www.phpmyadmin.net/home_page/security/PMASA-2009-2.php)
- Bulletin de sécurité phpMyAdmin PMASA-2009-3 du 24 mars 2009 :  
[http://www.phpmyadmin.net/home\\_page/security/PMASA-2009-3.php](http://www.phpmyadmin.net/home_page/security/PMASA-2009-3.php)
- Référence CVE CVE-2009-1148 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1148>
- Référence CVE CVE-2009-1149 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1149>
- Référence CVE CVE-2009-1150 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1150>
- Référence CVE CVE-2009-1151 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1151>

## Gestion détaillée du document

**26 mars 2009** version initiale.