



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 26 janvier 2006  
N° CERTA-2005-AVI-484-002

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-2005-AVI-484>

---

### Gestion du document

Référence	CERTA-2005-AVI-484-002
Titre	Vulnérabilité dans phpMyAdmin
Date de la première version	08 décembre 2005
Date de la dernière version	26 janvier 2006
Source(s)	Mise à jour de sécurité de phpMyAdmin du 07 décembre 2005
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 ;
- Cross Site Scripting ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

phpMyAdmin 2.x.

## 3 Résumé

Une vulnérabilité dans phpMyAdmin permet à un utilisateur mal intentionné de porter atteinte à la confidentialité des données, de réaliser des attaques de type Cross Site Scripting ou d'exécuter du code arbitraire à distance.

## 4 Description

Une vulnérabilité dans l'émulation `register_global` dans le fichier `grab_globals.php` permet à un utilisateur mal intentionné d'écraser la valeur de la variable `import_blacklist` afin d'exécuter du code arbitraire à distance sur les postes clients accédant au serveur compromis.

## 5 Solution

Appliquer la mise à jour de sécurité phpMyAdmin en passant à la version 2.7.0-pl1 disponible à l'adresse suivante :

[http://sourceforge.net/project/showfiles.php?group\\_id=23067](http://sourceforge.net/project/showfiles.php?group_id=23067)

## 6 Documentation

- Mise à jour de sécurité phpMyAdmin version 2.7.0-pl1 :  
[http://sourceforge.net/project/showfiles.php?group\\_id=23067](http://sourceforge.net/project/showfiles.php?group_id=23067)
- Bulletin de sécurité Hardened-PHP du 07 décembre 2005 :  
[http://www.hardened-php.net/advisory\\_252005.110.html](http://www.hardened-php.net/advisory_252005.110.html)
- Bulletin de sécurité phpMyAdmin PMASA-2005-8 du 05 décembre 2005 :  
[http://www.phpmyadmin.net/home\\_page/security.php?issue=PMASA-2005-8](http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2005-8)
- Bulletin de sécurité phpMyAdmin PMASA-2005-9 du 07 décembre 2005 :  
[http://www.phpmyadmin.net/home\\_page/security.php?issue=PMASA-2005-9](http://www.phpmyadmin.net/home_page/security.php?issue=PMASA-2005-9)
- Bulletin de sécurité Gentoo GLSA 200512-03 du 11 décembre 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200512-03.xml>
- Bulletin de sécurité FreeBSD pour phpMyAdmin du 07 décembre 2005 :  
<http://www.vuxml.org/freebsd/pkg-phpMyAdmin.html>
- Bulletin de sécurité SUSE SUSE-SA:2006:004 du 26 janvier 2006 :  
[http://www.novell.com/linux/security/advisories/2006\\_04\\_phpmyadmin.html](http://www.novell.com/linux/security/advisories/2006_04_phpmyadmin.html)
- Référence CVE CAN-2005-3665 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3665>
- Référence CVE CAN-2005-4079 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-4079>

## Gestion détaillée du document

**08 décembre 2005** version initiale.

**13 décembre 2005** ajout de la référence au bulletin de sécurité Hardened-PHP, ajout des références aux bulletins de sécurité phpMyAdmin PMASA-2005-8 et PMASA-2005-9, ajout des références aux bulletins de sécurité Gentoo GLSA 200512-03 et FreeBSD et ajout des références CVE CAN-2005-3665 et CAN-2005-4079.

**26 janvier 2006** ajout de la référence au bulletin de sécurité SUSE.