



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 10 mars 2006  
N° CERTA-2005-AVI-428-003

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans PHP

---

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-428>

---

### Gestion du document

Référence	CERTA-2005-AVI-428-003
Titre	Multiples vulnérabilités dans PHP
Date de la première version	02 novembre 2005
Date de la dernière version	10 mars 2006
Source(s)	Bulletins de sécurité du site Hardened-PHP Project
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

- Déni de service ;
- exécution de code arbitraire ;
- contournement de la politique de sécurité ;
- attaque de type « cross site scripting ».

## 2 Systèmes affectés

- PHP 4.0.x
- PHP 4.1.x
- PHP 4.2.x
- PHP 4.3.x
- PHP 4.4.x
- PHP 5.0.x

### 3 Résumé

Plusieurs vulnérabilités présentes dans PHP peuvent être exploitées par un utilisateur mal intentionné pour réaliser un déni de service, contourner la politique de sécurité, réaliser une attaque de type « cross site scripting » ou encore exécuter du code arbitraire sur le serveur où se trouve installée une version vulnérable de PHP.

### 4 Description

- La première vulnérabilité est présente lorsque la variable `register_globals` est activée. Cette vulnérabilité est due à un manque de protection sur le tableau `GLOBALS` contenant les variables globales du système. Un utilisateur peut exploiter cette vulnérabilité par l'envoi d'un fichier malicieusement construit ;
- une seconde vulnérabilité dans le traitement de la fonction `parse_str` peut-être exploitée pour activer le paramètre `registers_globals` ;
- une vulnérabilité due à l'absence de vérification des entrées passées dans la fonction `phpinfo` peut être utilisée par un utilisateur mal intentionné, via un script du même nom sur un serveur web malicieusement construit, pour exécuter un script arbitraire ou envoyer du code html arbitraire au cours d'une consultation par un navigateur tiers ;
- une vulnérabilité déjà citée dans l'avis CERTA-2005-AVI-336 sur la bibliothèque `pcrplib` peut être exploitée, via une expression régulière dans un script utilisant les fonctions php vulnérables, pour exécuter du code arbitraire sur le système vulnérable.

### 5 Solution

Appliquer les correctifs comme indiqué par l'éditeur (cf. Documentation).

### 6 Documentation

- Site Internet du hardened-php project :  
<http://www.hardened-php.net>
- Bulletin de sécurité 18/2005 du hardened-php project :  
[http://www.hardened-php.net/advisory\\_182005.77.html](http://www.hardened-php.net/advisory_182005.77.html)
- Bulletin de sécurité 19/2005 du hardened-php project :  
[http://www.hardened-php.net/advisory\\_192005.78.html](http://www.hardened-php.net/advisory_192005.78.html)
- Bulletin de sécurité 20/2005 du hardened-php project :  
[http://www.hardened-php.net/advisory\\_202005.79.html](http://www.hardened-php.net/advisory_202005.79.html)
- Mise à jour de PHP pour la version 4 :  
[http://www.php.net/release\\_4\\_4\\_1.php](http://www.php.net/release_4_4_1.php)
- Bulletin de sécurité CERTA-2005-AVI-336 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-336/>
- Bulletin de sécurité RedHat RHSA-2005:831 du 10 novembre 2005 :  
<https://rhn.redhat.com/errata/RHSA-2005-831.html>
- Bulletin de sécurité Gentoo GLSA 200511-08 du 13 novembre 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200511-08.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:213 du 16 novembre 2005 :  
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2005:213>
- Bulletin de sécurité SUSE SUSE-SA:2005:069 du 14 décembre 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_69\\_php.html](http://www.novell.com/linux/security/advisories/2005_69_php.html)
- Bulletin de sécurité Mandriva MDKSA-2006:035 du 07 février 2006 :  
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:035>
- Référence CVE CAN-2005-3388 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3388>
- Référence CVE CAN-2005-3389 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3389>

- Référence CVE CAN-2005-3390 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3390>
- Référence CVE CAN-2005-3391 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3391>
- Référence CVE CAN-2005-3392 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3392>

## **Gestion détaillée du document**

**02 novembre 2005** version initiale.

**21 novembre 2005** ajout des références CVE et des références aux bulletins de sécurité RedHat, Gentoo et Mandriva.

**15 décembre 2005** ajout de la référence au bulletin de sécurité SUSE.

**10 mars 2006** ajout de la référence au bulletin de sécurité Mandriva MDKSA-2006:035.