



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 2007  
N° CERTA-2007-AVI-060

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-2007-AVI-060>

---

### Gestion du document

Référence	CERTA-2007-AVI-060
Titre	Vulnérabilité dans PHP
Date de la première version	26 janvier 2007
Date de la dernière version	–
Source(s)	Fil de discussion Security Focus
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

PHP 5.2 et 4.4.

## 3 Résumé

Une vulnérabilité dans PHP permet à un attaquant de contourner la politique de sécurité.

## 4 Description

Une vulnérabilité dans PHP permet à un utilisateur local de passer outre les restrictions *safe\_mode* et *open\_basedir*, et donc de contourner la politique de sécurité.

## 5 Solution

Se référer aux mises à jour de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Une mise à jour provisoire est disponible sur le serveur CVS de PHP.

## 6 Documentation

- Mise à jour provisoire pour PHP 4.4 dans la base CVS du site PHP.net :  
<http://cvs.php.net/viewcvs.cgi/php-src/ext/session/session.c?r1=1.336.2.53.2.7&r2=1.336.2.53.2.8>
- Mise à jour provisoire pour PHP 5.2 dans la base CVS du site PHP.net :  
<http://cvs.php.net/viewcvs.cgi/php-src/ext/session/session.c?r1=1.417.2.8.2.17&r2=1.417.2.8.2.17>
- Référence CVE CVE-2006-6383 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6383>

## Gestion détaillée du document

**26 janvier 2007** version initiale.