



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 octobre 2004  
N° CERTA-2004-AVI-344

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-2004-AVI-344>

---

### Gestion du document

Référence	CERTA-2004-AVI-344
Titre	Multiples vulnérabilités dans PHP
Date de la première version	14 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA 200410-04 / PHP
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

- Atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- PHP 5.0
- PHP 5.0.1

## 3 Résumé

Deux vulnérabilités dans PHP permettent à un utilisateur mal intentionné à distance de porter atteinte à la confidentialité et à l'intégrité des données.

## 4 Description

PHP est un langage de script permettant la réalisation de pages web dynamiques. Deux vulnérabilités viennent d'être découvertes :

- Une première vulnérabilité est due à un mauvais traitement dans `php_variables.c`. Cette vulnérabilité permet à un utilisateur mal intentionné de prendre connaissance des informations présentes sur le système vulnérable.
- Une seconde vulnérabilité concerne la fonction `SAPI_POST_HANDLER_FUNC ( )` présente dans `rfc1867.c`, elle permet à un utilisateur mal intentionné de porter atteinte à l'intégrité des données.

## 5 Solution

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

## 6 Documentation

- Site Internet de PHP :  
<http://www.php.net>
- Bulletin de sécurité Gentoo GLSA 200410-04 / PHP :  
<http://www.gentoo.org/security/en/glsa/glsa-200410-04.xml>

## Gestion détaillée du document

14 octobre 2004 version initiale.