

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : 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-2009-AVI-083>

---

### Gestion du document

Référence	CERTA-2009-AVI-083
Titre	Vulnérabilités dans PHP
Date de la première version	03 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de la version PHP 5.2.9 du 26 février 2008
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

- Dénis de service ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

PHP 5.x.

## 3 Résumé

Plusieurs vulnérabilités sont présentes dans PHP, permettant à un utilisateur malveillant de réaliser un déni de service et de porter atteinte à la confidentialité des données.

## 4 Description

Plusieurs vulnérabilités sont présentes dans PHP :

- un défaut dans la décompression des archives zip permet à un utilisateur malveillant de provoquer un arrêt inopiné du serveur ;

- une erreur de traitement des chaînes malformées transmises à la fonction *json\_decode()* permet à un utilisateur malveillant de provoquer une erreur de segmentation ;
- un problème dans la fonction *explode()* permet à un utilisateur malveillant de provoquer un déni de service ;
- une erreur d'index de tableau dans la fonction *imageRotate()* est exploitable par un utilisateur malveillant pour lire toute la mémoire.

## 5 Solution

La version PHP 5.2.9 remédie à ces vulnérabilités.

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

## 6 Documentation

- Bulletin de la version PHP 5.2.9 du 26 février 2008 :  
<http://www.php.net/ChangeLog-5.php#5.2.9>
- Bulletin Mandriva MDVSA-2009:021 du 21 janvier 2009 :  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:021>
- Bulletin Mandriva MDVSA-2009:022 du 21 janvier 2009 :  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:022>
- Bulletin Mandriva MDVSA-2009:023 du 21 janvier 2009 :  
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:023>
- Référence CVE CVE-2008-3659 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3659>
- Référence CVE CVE-2008-5498 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5498>

## Gestion détaillée du document

**03 mars 2009** version initiale.