Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 décembre 2010
N° CERTA-2010-AVI-618

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilités dans PHP


Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-618

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2010-AVI-618 |
| Titre | Vulnérabilités dans PHP |
| Date de la première version | 17 décembre 2010 |
| Date de la dernière version | – |
| Source | Bulletin de version de PHP 5 du 16 décembre 2010 |
| 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 ;
- exécution de code arbitraire ;
- déni de service à distance ;
- déni de service ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

PHP 5.2.x et 5.3.x.

## 3 Résumé

Plusieurs vulnérabilités affectent PHP. Certaines d'entre elles permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

# 4 Description

Plusieurs vulnérabilités affectent PHP :

- certaines erreurs dans le traitement des archives ZIP permettent de provoquer un déni de service à distance ;
- le traitement défectueux des archives PHP (adresses `phar://`) permet à un utilisateur malveillant de lire des données sensibles ou d'exécuter du code arbitraire à distance ;
- l'utilisation d'un nom de fichiers d'une certaine forme permet d'outrepasser les restrictions mises en place à l'aide du module *open_basedir* ;
- l'utilisation d'une adresse mèl d'une certaine forme permet de provoquer un déni de service par épuisement de la mémoire ;
- une double désallocation de mémoire permet à un utilisateur malveillant de provoquer un déni de service. La possibilité d'exécuter du code arbitraire n'est pas exclue.

# 5 Solution

Les versions 5.3.4, 5.2.15 et 5.2.16 de PHP remédient à ces vulnérabilités.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

# 6 Documentation

- Bulletin de version de PHP 5 du 16 décembre 2010 :
  http://www.php.net/ChangeLog-5.php
- Référence CVE CVE-2010-2950 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2950
- Référence CVE CVE-2010-3436 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3436
- Référence CVE CVE-2010-3709 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3709
- Référence CVE CVE-2010-3710 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3710
- Référence CVE CVE-2010-4150 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4150

# Gestion détaillée du document

**17 décembre 2010** version initiale.