



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 septembre 2007
N° CERTA-2007-AVI-388

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-2007-AVI-388>

Gestion du document

Référence	CERTA-2007-AVI-388
Titre	Multiples vulnérabilités dans PHP
Date de la première version	05 septembre 2007
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 5.2.4 de PHP du 30 août 2007
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

PHP versions 5.2.3 et antérieures.

3 Résumé

De multiples vulnérabilités sont présentes dans PHP et permettent à un utilisateur distant d'exécuter du code arbitraire ou de contourner la politique de sécurité du site mis en œuvre avec PHP.

4 Description

Plusieurs failles sont présentes dans PHP :

- une erreur d'impact non précisé par l'éditeur a été identifiée dans la fonction `money_format()` ;

- une seconde dans la fonction `zend_alter_ini_entry()` permet de déclencher une interruption arbitraire ;
- plusieurs failles de type débordement de mémoire dans la mise en œuvre de la bibliothèque de fonctions GD par PHP permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire ;
- une erreur dans la mise en œuvre de requêtes SQL sur un serveur MySQL dans PHP permet à un utilisateur de contourner les restrictions associées aux directives `open_basedir` et `safe_mode` ;
- un manque de contrôle dans la fonction `glob` permet également de contourner les restrictions de `open_basedir` ;
- une dernière vulnérabilité relative à l'extension `session` permet de contourner les restrictions de `open_basedir` si le fichier de session est un lien symbolique.

5 Solution

La version 5.2.4 de PHP corrige le problème :

<http://www.php.net/downloads.php>

6 Documentation

- Site de PHP :
<http://www.php.net>
- Liste des changements apportés à la version 5.2.4 de PHP :
http://www.php.net/releases/5_2_4.php
- Référence CVE CVE-2007-3996 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3996>
- Référence CVE CVE-2007-3378 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3378>
- Référence CVE CVE-2007-3997 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3997>

Gestion détaillée du document

05 septembre 2007 version initiale.