

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-2010-AVI-092>

Gestion du document

Référence	CERTA-2010-AVI-092
Titre	Multiples vulnérabilités dans PHP
Date de la première version	01 mars 2010
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 5.2.13 de PHP du 25 février 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

Contournement de la politique de sécurité.

2 Systèmes affectés

PHP versions 5.2.12 et antérieures.

3 Résumé

Plusieurs vulnérabilités présentes dans PHP permettent à un utilisateur distant de contourner la politique de sécurité.

4 Description

Le *Safe Mode* de PHP est une option de configuration qui permet d'augmenter le nombre de contrôles faits lors de l'appel à certaines commandes du langage jugées comme dangereuses. On trouve parmi ces commandes, par exemple : *exec()*, *system()* ou encore *fpopen()*.

Deux vulnérabilités ont été identifiées dans ce *Safe Mode* de PHP :

- la première concerne la directive *open_basedir* du *Safe Mode* qui peut être contournée sous certaines conditions ;
- la seconde est relative à un manque de contrôle sur la fonction *tempnam()*.

Ces deux vulnérabilités permettent à un utilisateur distant de mettre en défaut certaines protections mises en œuvre dans le *Safe Mode*.

Remarque :

Selon le projet PHP (www.php.net), le *Safe Mode* est considéré comme obsolète depuis la sortie de la version 5.3.0 et ne sera plus présent dans les prochaines versions du langage.

5 Solution

La version 5.2.13 de PHP corrige le problème :

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

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

6 Documentation

- Site du projet PHP :
<http://www.php.net>
- Liste des changements apportés à la version 5.2.13 de PHP du 25 février 2010 :
<http://www.php.net/ChangeLog-5.php#5.2.13>

Gestion détaillée du document

01 mars 2010 version initiale.