Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 décembre 2009
N° CERTA-2009-AVI-553

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de PHP

Gestion du document

Référence	CERTA-2009-AVI-553
Titre	Multiples vulnérabilités de PHP
Date de la première version	18 décembre 2009
Date de la dernière version	–
Source(s)	Notes de mise à jour PHP 5.2.12
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

- Déni de service à distance ;
- contournement de la politique de sécurité ;
- injection de code indirecte.

2 Systèmes affectés

PHP versions 5.2.11 et antérieures.

3 Résumé

De multiples vulnérabilités ont été découvertes dans PHP. L'exploitation de ces vulnérabilités permet de réaliser des actions diverses dont le déni de service à distance ou la contournement de certains mécanismes de sécurité.

4 Description

Cinq vulnérabilités ont été découvertes dans `PHP` :

- la première est due à une erreur dans la fonction *tempnam()*, permettant de contourner le mécanisme de *safe_mode* ;
- la deuxième est due à une erreur dans la fonction *posix_mkfifo()*, permettant de contourner la fonctionalité *open_basedir* ;
- la troisième est due à une erreur dans la gestion du chargement de certaines données et peut être utilisée afin de provoquer un déni de service ;
- la quatrième est due à une mauvaise gestion des sessions (l'impact n'est pas connu) ;
- la dernière est due à une erreur au niveau de la fonction *htmlspecialchars()* et permet à un utilisateur mal intentionné de réaliser une injection de code indirecte.

5 Solution

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

6 Documentation

- Notes de mise à jour PHP 5.2.12 :
  http://www.php.net/releases/5_2_12.php
- Référence CVE CVE-2009-3557 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3557
- Référence CVE CVE-2009-3558 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3558
- Référence CVE CVE-2009-4017 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4017
- Référence CVE CVE-2009-4142 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4142
- Référence CVE CVE-2009-4143 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4143

Gestion détaillée du document

18 décembre 2009 version initiale.