



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 novembre 2009
N° CERTA-2009-AVI-510-001

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-2009-AVI-510>

Gestion du document

| | |
|-----------------------------|--------------------------------------|
| Référence | CERTA-2009-AVI-510-001 |
| Titre | Multiples vulnérabilités dans PHP |
| Date de la première version | 23 novembre 2009 |
| Date de la dernière version | 27 novembre 2009 |
| Source(s) | Bulletin de mise à jour de PHP 5.3.1 |
| 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de PHP antérieures à la 5.3.1.

3 Résumé

Plusieurs vulnérabilités affectant PHP ont été corrigées. Elles permettent, entre autre, de contourner la politique de sécurité.

4 Description

Plusieurs vulnérabilités dans PHP permettant, entre autre, le contournement de la politique de sécurité ont été corrigées. Une personne malveillante peut par exemple, à l'aide d'un fichier spécialement réalisé, créer des fichiers dans les répertoires autorisés en écriture.

5 Solution

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

6 Documentation

- Bulletin de mise à jour de PHP 3.5.1 :
http://www.php.net/releases/5_3_1.php
- Bulletin de sécurité Debian DSA-1940 du 13 novembre 2009 :
<http://www.debian.org/security/2009/dsa-1940>
- Bulletin de sécurité SuSE SUSE-SR:2009:017 du 26 octobre 2009 :
<http://lists.opensuse.org/opensuse-security-announce/2009-10/msg00004.html>
- Référence CVE CVE-2009-3292 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3292>
- 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>

Gestion détaillée du document

23 novembre 2009 version initiale.

27 novembre 2009 ajout des références CVE et des bulletins de sécurité Debian et SuSE.