

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2012-AVI-021>

Gestion du document

Référence	CERTA-2012-AVI-021
Titre	Vulnérabilités dans PHP
Date de la première version	16 janvier 2012
Date de la dernière version	–
Source	Liste des changements de la version 5.3.9 de PHP du 10 janvier 2012
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

- Dénis de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

PHP, versions antérieures à la version 5.3.9

3 Résumé

Plusieurs vulnérabilités de PHP permettent à un attaquant de provoquer un déni de service à distance ou de lire indûment des données.

4 Description

PHP présente des vulnérabilités :

- le système de calcul de condensats pour les formulaires permet de provoquer un déni de service à distance par épuisement des ressources processeur ;

- sur les systèmes en 32 bits, le traitement defectueux d'en-têtes EXIF permet à un attaquant de lire des zones de la mémoire pour lesquelles il ne dispose pas des droits ou de provoquer un arrêt inopiné du système.

5 Solution

La version PHP 5.3.9 corrige ces problèmes.

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

6 Documentation

- Liste des changements de la version 5.3.9 de PHP du 10 janvier 2012 :
<http://www.php.net/Change-Log5.php>
- Note de vulnérabilité de l'US-CERT VU#903934 du 30 décembre 2011 :
<http://www.kb.cert.org/vuls/id/903934>
- Référence CVE CVE-2011-4566 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4566>
- Référence CVE CVE-2011-4885 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4885>

Gestion détaillée du document

16 janvier 2012 version initiale.