

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-2011-AVI-160>

Gestion du document

Référence	CERTA-2011-AVI-160-001
Titre	Vulnérabilités dans PHP
Date de la première version	22 mars 2011
Date de la dernière version	23 mars 2011
Source	Annonce de version de PHP du 17 mars 2011
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 ;
- déni de service ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

PHP version 5.3.5 et versions 5.3.x antérieures.

3 Résumé

Plusieurs vulnérabilités sont présentes dans PHP et permettent, en particulier, à un utilisateur malveillant d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités sont présentes dans PHP :

- un argument est traité de manière incorrecte par la fonction `_zip_name_locate()`. Ce défaut permet de provoquer un arrêt inopiné de l'application ;

- un transtypage incorrect sur les architectures 64 bits dans l'extension Exif permet de provoquer un arrêt inopiné au moyen d'une image spécialement conçue ;
- un argument de la fonction *shmop_read()* est traité de manière incorrecte. Cette erreur est exploitable par un utilisateur malveillant pour provoquer un arrêt inopiné ou pour lire sans droit des données en mémoire ;
- des erreurs dans le traitement des formats de chaîne par les fonctions du fichier *phar_object.c* permettent à un utilisateur malveillant de provoquer un déni de service ou d'exécuter du code arbitraire ;
- une erreur de signe dans une variable du programme *zip_stream.c* est exploitable pour provoquer une consommation de 100% du CPU ;
- une erreur de traitement des archives par la fonction *stream_get_contents()* est exploitable pour provoquer un arrêt inopiné de l'application ;
- dans certaines circonstances, le traitement des URL de la forme ftp:// peut servir à provoquer un déni de service ;
- des fuites de mémoire de l'extension OpenSSL permettent de provoquer un épuisement des ressources mémoire ;
- un problème dans les conversions entre calendriers peut servir à provoquer un déni de service ;
- un débordement de zone mémoire dans la fonction *strval()* peut servir à provoquer un déni de service ;
- une erreur dans le formatage des nombres peut servir à provoquer un déni de service.

5 Solution

La version 5.3.6 de PHP corrige ces vulnérabilités.

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

6 Documentation

- Annonce de version de PHP du 17 mars 2011 :
<http://www.php.net/archive/2011.php#id2011-03-17-1>
- Référence CVE CVE-2011-0421 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0421>
- Référence CVE CVE-2011-0708 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0708>
- Référence CVE CVE-2011-1092 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1092>
- Référence CVE CVE-2011-1153 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1153>
- Référence CVE CVE-2011-1464 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1464>
- Référence CVE CVE-2011-1466 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1466>
- Référence CVE CVE-2011-1467 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1467>
- Référence CVE CVE-2011-1468 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1468>
- Référence CVE CVE-2011-1469 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1469>
- Référence CVE CVE-2011-1470 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1470>
- Référence CVE CVE-2011-1471 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1471>

Gestion détaillée du document

22 mars 2011 version initiale.

23 mars 2011 ajout de vulnérabilités et des CVE.