Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 octobre 2006
N° CERTA-2006-AVI-433

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans PHP

Gestion du document

Référence	CERTA-2006-AVI-433
Titre	Vulnérabilité dans PHP
Date de la première version	10 octobre 2006
Date de la dernière version	–
Source(s)	
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 à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- les versions PHP 4.x, antérieures à 4.3.0 ;
- les versions PHP 5.x, antérieures ou égales à la 5.1.6.

3 Résumé

Une vulnérabilité a été identifiée dans PHP. Celle-ci permettrait à une personne malveillante distante d'exécuter des commandes arbitraires sur le serveur Web vulnérable.

4 Description

PHP (venant de l'acronyme récursif *PHP: Hypertext Preprocessor*) est un langage généralement interprété par un serveur Web, afin de générer des documents comme des pages HTML.

Une vulnérabilité a été identifiée dans celui-ci. Elle concerne la fonction `unserialize()` se trouvant dans le fichier `zend_alloc.c`. Cette fonction fait appel à une autre fonction, nommée `ecalloc()`, qui ne vérifierait pas correctement certaines données avant d'allouer la mémoire. Une personne malveillante pourrait injecter des données afin de provoquer un débordement de cette mémoire et parvenir à exécuter des commandes arbitraires sur le serveur Web vulnérable. Cela est notamment rendu possible par les valeurs de variables `Cookie` envoyées au serveur.

Tout code PHP faisant appel à la fonction `unserialize()` serait vulnérable. Cela inclut en particulier plusieurs applications Web, dont phpBB, Invision Board, vBulletin, Serendpity, dotclear, etc.

5 Solution

Se référer aux mises à jour des éditeurs pour l'obtention des correctifs (cf. section Documentation). Une mise à jour provisoire est disponible sur le serveur CVS de PHP, ainsi que sur le site Hardened-PHP.

6 Documentation

- Ajout dans la base CVS du site PHP.net d'une mise à jour provisoire :
  http://cvs.php.net/viewvc.cgi/ZendEngine2/zend_alloc.c?r1=1.161&r2=1.162
- Bulletin de sécurité publié par le site Hardened-PHP du 09 octobre 2006 :
  http://www.hardened-php.net/advisory_092006.133.html
- Mise à jour provisoire fournie par le site Hardened-PHP :
  http://www.hardened-php.net/files/CVE-2006-4812.patch
- Bulletin de sécurité Mandriva MDKSA-2006:180 du 05 octobre 2006 :
  http://archives.mandrivalinux.com/security-announce/2006-10/msg00004.php
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:180
- Bulletin de sécurité RedHat RHSA-2006:0708 du 05 octobre 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0708.html
- Référence CVE CVE-2006-4812 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4812

Gestion détaillée du document

10 octobre 2006 version initiale.