Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 août 2008
N° CERTA-2008-AVI-417

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans PHP

Gestion du document

Référence	CERTA-2008-AVI-417
Titre	Multiples vulnérabilités dans PHP
Date de la première version	14 août 2008
Date de la dernière version	–
Source(s)	Note de changement de version PHP 4.4.9 du 07 août 2008
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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Les versions PHP de la branche 4 antérieures à 4.4.9.

Cette branche ne devrait plus être maintenue à la fin de l'année 2008.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans PHP 4. Leur exploitation permettrait de perturber le système ou de récupérer des données confidentielles.

4 Description

Plusieurs vulnérabilités ont été identifiées dans PHP 4 :

- la bibliothèque PCRE (*Perl-Compatible Regular Expression*) ne gère pas correctement certaines expressions régulières pouvant provoquer un débordement de pile ;
- la fonction `memnstr()` appelée par `explode()` ne contrôlerait pas correctement certaines entrées ;
- la fonction `imageloadfont()` (gd/ext) ne gère pas convenablement certains caractères ;
- PHP ne manipulerait pas correctement certains liens avec des points multiples de type `XXX..php` ;
- il est possible de contourner le `safe_mode` sous certaines conditions.
- l'extension curl ne manipulerait pas correctement l'option `open_basedir`.

Certaines de ces vulnérabilités ont fait l'objet d'un correctif dans la branche 5 en juin 2008 et sont mentionnées dans l'avis CERTA-2008-AVI-225.

5 Solution

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

6 Documentation

- Note de changement de version PHP 4.4.9 du 07 août 2008 :
  http://www.php.net/ChangeLog-4.php#4.4.9
- Commentaires de rapport de bogues Gentoo du 06 août 2008 :
  http://bugs.gentoo.org/show_bug.cgi?id=234102
- Avis du CERTA CERTA-2008-AVI-225 du 25 juin 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-225/
- Référence CVE CVE-2008-2371 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2371
- Référence CVE CVE-2008-2665 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2665
- Référence CVE CVE-2008-2666 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2666

Gestion détaillée du document

14 août 2008 version initiale.