Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juin 2008
N° CERTA-2008-AVI-225-001

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-2008-AVI-225

Gestion du document

Référence	CERTA-2008-AVI-225-001
Titre	Multiples vulnérabilités dans PHP
Date de la première version	02 mai 2008
Date de la dernière version	25 juin 2008
Source(s)	Notes de version PHP 5.2.6 du 01 mai 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

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

`PHP` versions 5.2.5 et antérieures.

3 Résumé

De multiples vulnérabilités dans `PHP 5` permettent l'exécution de code arbitraire à distance et le contournement de la politique de sécurité.

4 Description

De multiples vulnérabilités ont été découvertes dans `PHP`. L'une d'entre elles permet de contourner le mode `safe_mode`. D'autres failles permettent l'exécution de code arbitraire à distance.

5 Solution

Mettre `PHP` à jour en version 5.2.6 (cf. section Documentation).

6 Documentation

- Version 5.2.6 de PHP :
  http://www.php.net/downloads.php#v5
- Notes de version PHP 5.2.6 du 01 mai 2008 :
  http://www.php.net/ChangeLog-5.php
- Bulletin de sécurité Fedora FEDORA-2008-3864 du 20 juin 2008 :
  https://www.redhat.com/archives/fedora-package-announce/2008-june/msg00773.html
- Référence CVE CVE-2008-0599 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0599
- Référence CVE CVE-2008-2051 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2051
- Référence CVE CVE-2008-2107 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2107
- Référence CVE CVE-2008-2108 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2108

Gestion détaillée du document

02 mai 2008 version initiale.

25 juin 2008 ajout des références aux CVE et au bulletin de sécurité Fedora.