Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 février 2005
N° CERTA-2004-AVI-405-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de PHP

Gestion du document

Référence	CERTA-2004-AVI-405-004
Titre	Multiples vulnérabilités de PHP
Date de la première version	20 décembre 2004
Date de la dernière version	17 février 2005
Source(s)	Bulletin de sécurité PHP
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

- atteinte à la disponibilité des données et du système ;
- atteinte à l'intégrité des données et du système ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- PHP versions 4.3.9 et antérieures ;
- PHP versions 5.0.2 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans PHP permettent à un utilisateur distant mal intentionné de porter atteinte à la disponibilité, la confidentialité et à l'intégrité des données et/ou du système les hébergeant.

4 Description

PHP est un langage de script permettant la réalisation de pages web dynamiques.
De multiples vulnérabilités sont présentes dans PHP :

- CVE CAN-2004-1018 : une vulnérabilité de type débordement de mémoire est présente dans les fonctions `pack()` et `unpack()`. Sous certaines conditions, il est possible pour un utilisateur distant mal intentionné de réaliser l'exécution de code arbitraire avec les privilèges du serveur Web ;
- CVE CAN-2004-1019 : de multiples vulnérabilités dans la fonction `unserialize()` peuvent être exploitées pour un accès non autorisé à des données ou l'exécution de code arbitraire ;
- CVE CAN-2004-1020 : la fonction `addslashes()` ne traitant pas correctement certains caractères en entrée, il est possible pour un utilisateur distant mal intentionné de lire ou d'écraser des fichiers arbitraires sur le système ;
- CVE CAN-2004-1063 : il est possible, sous certaines conditions, de contourner les restrictions d'accès mises en place avec `safe_mode` ;
- CVE CAN-2004-1064 : certaines mises en oeuvre de la fonction `realpath` ne traitent pas correctement des chemins d'accès long. Il est possible, sous certaines conditions, de réaliser l'inclusion arbitraire de fichiers ;

5 Solution

Les versions 4.3.10 et 5.0.3 corrigent ces vulnérabilités.
Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs.

6 Documentation

- Site de PHP :
  http://www.php.net
- Annonce de la sortie de la version 4.3.10 de PHP :
  http://www.php.net/release_4_3_10_fr.php
- Bulletin de sécurité Mandrake MDKSA-2004:151 du 17 décembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:151
- Bulletin de sécurité Gentoo GLSA-200412-14 du 19 décembre 2004 :
  http://www.gentoo.org/security/glsa/glsa-200412-14.xml
- Bulletin de sécurité Red Hat RHSA-2004:687 du 21 décembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-687.html
- Bulletin de sécurité Red Hat RHSA-2005:031 du 19 janvier 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-031.html
- Bulletin de sécurité Red Hat RHSA-2005:032 du 15 février 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-032.html
- Bulletin de sécurité FreeBSD du 17 décembre 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité OpenBSD du 18 décembre 2004 :
  http://www.vuxml.org/openbsd/
- Bulletin de sécurité OpenBSD du 20 décembre 2004 relatif à PHP5:
  http://www.vuxml.org/openbsd/
- Bulletin de sécurité SUSE SuSE-SA:2005:002 du 17 janvier 2005 :
  http://www.novell.com/linux/security/advisories/2005_02_php4_mod_php4.html
- Référence CVE CAN-2004-1018 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1018
- Référence CVE CAN-2004-1019 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1019
- Référence CVE CAN-2004-1020 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1020
- Référence CVE CAN-2004-1063 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1063

- Référence CVE CAN-2004-1064 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1064
- Référence CVE CAN-2004-1065 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1065

Gestion détaillée du document

20 décembre 2004 version initiale.
22 décembre 2004 ajout références aux bulletins de sécurité Red Hat et OpenBSD (PHP5).
24 janvier 2005 ajout référence au bulletin de sécurité Red Hat.
17 février 2005 ajout référence au bulletin de sécurité Red Hat RHSA-2005-032.