



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 mai 2007
N° CERTA-2007-AVI-201-001

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-2007-AVI-201>

Gestion du document

Référence	CERTA-2007-AVI-201-001
Titre	Multiples vulnérabilités dans PHP
Date de la première version	07 mai 2007
Date de la dernière version	29 mai 2007
Source(s)	Bulletins des mises à jour PHP du 03 mai 2007
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- PHP 4, pour les versions antérieures à 4.4.7 ;
- PHP 5, pour les versions antérieures à 5.2.2.

3 Résumé

Plusieurs vulnérabilités avaient été identifiées à l'occasion du MoPB (le *Month Of PHP Bugs*). L'exploitation de ces dernières peut avoir divers impacts sur le serveur vulnérable. Les mises à jour récentes de PHP corrigent la plupart de ces vulnérabilités.

4 Description

Plusieurs vulnérabilités avaient été identifiées en mars 2007 à l'occasion du MOPB (le *Month Of PHP Bugs*). A cette occasion, le CERTA a publié dans son bulletin d'actualité CERTA-2007-ACT-012 une revue des plus importantes d'entre elles. Les conséquences de l'exploitation de ces dernières sont diverses, pouvant être un dysfonctionnement du serveur vulnérable ou l'exécution de code arbitraire sur celui-ci.

5 Solution

Se référer aux bulletins de sécurité des différents éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin d'actualité CERTA-2007-ACT-012 du 23 mars 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-012.pdf>
- Note de changement de version pour PHP 4 version 4.4.7 :
<http://www.php.net/ChangeLog-4.php>
- Note de changement de version pour PHP 5 version 5.2.2 :
<http://www.php.net/ChangeLog-5.php>
- Site de téléchargement des dernières versions PHP :
<http://fr2.php.net/downloads.php>
- Bulletin de sécurité Debian DSA 1282-1 du 26 avril 2007 :
<http://www.debian.org/security/2007/dsa-1282-1>
- Bulletin de sécurité Debian DSA 1283-1 du 29 avril 2007 :
<http://www.debian.org/security/2007/dsa-1283-1>
- Mise à jour de sécurité Fedora Core 6 du 18 avril 2007 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/6/>
- Bulletin de sécurité Mandriva MDKSA-2007:087 du 18 avril 2007 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:087>
- Bulletin de sécurité Mandriva MDKSA-2007:088 du 18 avril 2007 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:088>
- Bulletin de sécurité Mandriva MDKSA-2007:089 du 18 avril 2007 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:089>
- Bulletin de sécurité Mandriva MDKSA-2007:090 du 18 avril 2007 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:090>
- Bulletin de sécurité Mandriva MDKSA-2007:091 du 18 avril 2007 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:091>
- Bulletin de sécurité RedHat RHSA-2007:0153 du 20 avril 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0153.html>
- Bulletin de sécurité RedHat RHSA-2007:0155 du 16 avril 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0155.html>
- Bulletin de sécurité Ubuntu USN-455-1 du 27 avril 2007 :
<http://www.ubuntu.com/usn/usn-455-1>
- Bulletin de sécurité Gentoo GLSA-200705-19 du 26 mai 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200705-19.xml>
- Bulletin de sécurité SuSE SUSE-SA:2007:032 du 23 mai 2007 :
<http://lists.suse.com/archive/suse-security-announce/2007-May/0007.html>
- Référence CVE CVE-2007-0455 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0455>
- Référence CVE CVE-2007-1001 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1001>
- Référence CVE CVE-2007-1286 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1286>

- Référence CVE CVE-2007-1375 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1375>
- Référence CVE CVE-2007-1376 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1376>
- Référence CVE CVE-2007-1380 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1380>
- Référence CVE CVE-2007-1453 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1453>
- Référence CVE CVE-2007-1454 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1454>
- Référence CVE CVE-2007-1521 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1521>
- Référence CVE CVE-2007-1583 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1583>
- Référence CVE CVE-2007-1700 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1700>
- Référence CVE CVE-2007-1711 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1711>
- Référence CVE CVE-2007-1718 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1718>
- Référence CVE CVE-2007-1777 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1777>
- Référence CVE CVE-2007-1824 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1824>
- Référence CVE CVE-2007-1887 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1887>
- Référence CVE CVE-2007-1889 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1889>
- Référence CVE CVE-2007-1900 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1900>

Gestion détaillée du document

07 mai 2007 version initiale.

29 mai 2007 ajout des références aux bulletins de sécurité Gentoo, SuSE, Mandriva, Red Hat.