

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-076>

Gestion du document

Référence	CERTA-2007-AVI-076-003
Titre	Multiples vulnérabilités dans php
Date de la première version	09 février 2007
Date de la dernière version	15 mars 2007
Source(s)	Liste des correctifs apportés à la version 5.2.1 de 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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

php versions 5.2.0 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans php permettraient à un utilisateur distant de contourner la politique de sécurité ou de porter atteinte à la confidentialité des données.

4 Description

Plusieurs vulnérabilités de type débordement de mémoire dans l'interpréteur php ont été identifiées. Elles permettraient de contourner la politique de sécurité et de porter atteinte à la confidentialité des données du système mettant en œuvre cet interpréteur php vulnérable.

5 Solution

La version 5.2.1 de `php` corrige le problème :
<http://www.php.net/downloads.php>

6 Documentation

- Liste des correctifs apportés à la version 5.2.1 de `php` :
http://www.php.net/releases/5_2_1.php
- Bulletin de sécurité SuSE SUSE-SA:2007:00 :
<http://lists.suse.com/archive/suse-security-announce/2007-Mar/0003.html>
- Bulletin Redhat RHSA-2007:0076-3 du 19 février 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0076.html>
- Bulletin Redhat RHSA-2007:0081-2 du 21 février 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0081.html>
- Référence CVE CVE-2007-0905 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0905>
- Référence CVE CVE-2007-0906 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0906>
- Référence CVE CVE-2007-0907 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0907>
- Référence CVE CVE-2007-0908 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0908>
- Référence CVE CVE-2007-0909 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0909>
- Référence CVE CVE-2007-0910 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0910>
- Référence CVE CVE-2007-0988 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0988>
- Bulletin Debian DSA-1264-1 du 07 mars 2007 :
<http://www.debian.org/security/2007/dsa-1264>
- Bulletin Mandriva MDKSA-2007:048 du 22 février 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:048>
- Bulletin Ubuntu USN-424-1 du 21 février 2007 :
<https://lists.ubuntu.com/archives/ubuntu-security-announce/2007-February/000487.html>
- Bulletin Ubuntu USN-424-2 du 08 mars 2007 :
<https://lists.ubuntu.com/archives/ubuntu-security-announce/2007-March/000497.html>
- Bulletin Fedora Core 5 Fedora-2007-287 du 26 février 2007 :
<http://fedoranews.org/cms/node/2720>
- Bulletin Fedora Core 6 Fedora-2007-261 du 20 février 2007 :
<http://fedoranews.org/cms/node/2681>

Gestion détaillée du document

09 février 2007 version initiale.

21 février 2007 ajout des références CVE et Redhat.

14 mars 2007 ajout des références Debian, Fedora, Mandriva et Redhat.

15 mars 2007 ajout de la référence SuSE.