Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mars 2007
N° CERTA-2007-AVI-144

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans PHP

Gestion du document

Référence	CERTA-2007-AVI-144
Titre	Multiples vulnérabilités dans PHP
Date de la première version	27 mars 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA-200703-21 du 20 mars 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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- PHP antérieur à la version 4.4.5 ;
- PHP antérieur à la version 5.2.1.

3 Résumé

Plusieurs vulnérabilités découvertes dans PHP (PHP : Hypertext Processor) permettent à un utilisateur distant malintentionné de réaliser de nombreuses actions malveillantes sur le système vulnérable.

Ces vulnérabilités peuvent être exploitées à distance afin de contourner la politique de sécurité, d'exécuter du code arbitraire, de provoquer un déni de service en consommant de façon excessive les ressources du processeur et de porter atteinte à la confidentialité et à l'intégrité des données du système présentes en mémoire.

4 Solution

Appliquer les mises à jour de sécurité PHP en passant à la version 4.4.5 ou 5.2.1 disponibles aux adresses suivantes :
http://www.php.net/releases/4_4_5.php
http://www.php.net/releases/5_2_1.php

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

5 Documentation

- Mise à jour de sécurité PHP version 4.4.5 :
  http://www.php.net/releases/4_4_5.php
- Mise à jour de sécurité PHP version 5.2.1 :
  http://www.php.net/releases/5_2_1.php
- Bulletin de sécurité Debian DSA 1264 du 07 mars 2007 :
  http://www.debian.org/security/2007/dsa-1264
- Bulletin de sécurité Gentoo GLSA-200703-21 du 20 mars 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200703-21.xml
- Bulletin de sécurité Mandriva MDKSA-2007:048 du 22 février 2007 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2007:048
- Bulletin de sécurité RedHat RHSA-2007:0089 du 26 février 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0089.html
- Bulletin de sécurité RedHat RHSA-2007:0081 du 21 février 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0081.html
- Bulletin de sécurité RedHat RHSA-2007:0076 du 19 février 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0076.html
- Bulletin de sécurité SuSE SUSE-SA:2007:020 du 15 mars 2007 :
  http://lists.suse.com/archive/archive/suse-security-announce/2007-Mar/0003.html
- Bulletin de sécurité Ubuntu USN-423-1 du 20 février 2007 :
  http://www.ubuntulinux.org/usn/usn-423-1
- Bulletin de sécurité Ubuntu USN-431-1 du 07 mars 2007 :
  http://www.ubuntulinux.org/usn/usn-431-1
- Bulletin de sécurité Avaya ASA-2007-0076 du 06 mars 2007 :
  http://support.avaya.com/elmodocs2/security/ASA-2007-0076.htm
- Bulletin de sécurité Avaya ASA-2007-0088 du 26 mars 2007 :
  http://support.avaya.com/elmodocs2/security/ASA-2007-0088.htm
- 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
- 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-2007-1383 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1383
- Référence CVE CVE-2007-1452 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1452
- 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

Gestion détaillée du document

27 mars 2007 version initiale.