

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-2005-AVI-126>

Gestion du document

Référence	CERTA-2005-AVI-126-002
Titre	Multiples vulnérabilités dans PHP
Date de la première version	01 avril 2005
Date de la dernière version	17 juin 2005
Source(s)	Mise à jour de sécurité PHP 4.3.11 du 01 avril 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Déni de service.

2 Systèmes affectés

- PHP 4.2.x ;
- PHP 4.3.x ;
- PHP 5.0.x.

3 Résumé

Deux vulnérabilités dans PHP permettent à un utilisateur mal intentionné d'effectuer un déni de service à distance sur la plate-forme vulnérable.

4 Description

PHP est un langage de script permettant la réalisation de pages web dynamiques.

Deux vulnérabilités découvertes dans les fonctions `php_handle_iff()` et `php_handle_jpeg()` peuvent être exploitées par un individu mal intentionné, au moyen d'une image malicieusement construite afin de consommer toutes les ressources CPU du système.

5 Solution

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

6 Documentation

- Site Internet de l'éditeur :
<http://www.php.net>
- Bulletin de sécurité iDEFENSE #222 du 31 mars 2005 :
<http://www.idefense.com/application/poi/display?id=222&type=vulnerabilities>
- Bulletin de sécurité PHP du 01 avril 2005 :
http://www.php.net/release_4_3_11.php
- Mise à jour de sécurité PHP 4.3.11 du 01 avril 2005 :
<http://www.php.net/downloads.php>
- Bulletin de sécurité Debian DSA-708 du 15 avril 2005 :
<http://www.debian.org/security/2005/dsa-708>
- Bulletin de sécurité Debian DSA-729 du 26 mai 2005 :
<http://www.debian.org/security/2005/dsa-729>
- Bulletin de sécurité Mandriva MDKSA-2005:072 du 18 avril 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:072>
- Bulletin de sécurité Gentoo GLSA 200504-15/php du 18 avril 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200504-15.xml>
- Bulletin de sécurité RedHat RHSA-2005:405 du 28 avril 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-405.html>
- Bulletin de sécurité RedHat RHSA-2005:406 du 04 mai 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-406.html>
- Bulletin de sécurité Avaya ASA-2005-136 du 14 juin 2005 :
http://support.avaya.com/elmodocs2/security/ASA-2005-136_RHSA-2005-405_RHSA-2005-406.pdf
- Référence CVE CAN-2005-0524 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0524>
- Référence CVE CAN-2005-0525 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0525>

Gestion détaillée du document

01 avril 2005 version initiale.

27 mai 2005 ajout des références aux bulletins de sécurité Debian, Mandriva, Gentoo et RedHat.

17 juin 2005 ajout du bulletin de sécurité Avaya ASA-2005-136.