

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-242>

Gestion du document

Référence	CERTA-2005-AVI-242-009
Titre	Vulnérabilités dans PHP PEAR
Date de la première version	01 juillet 2005
Date de la dernière version	18 juillet 2005
Source(s)	
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.

2 Systèmes affectés

Tous les systèmes exploitant PHP PEAR pour leurs applications.

3 Description

Une vulnérabilité, jugée critique, a été découverte dans l'implémentation PEAR XMLRPC de PHP. Cette vulnérabilité fait déjà l'objet de publications de code permettant son exploitation.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).
Mettre à jour les applications PHP, dont les plus populaires disposent d'un correctif («WordPress» et «Serendipity»).

5 Documentation

- Bulletin de sécurité de Hardened-PHP du 29 juin 2005 :
<http://www.hardened-php.net/advisory-022005.php>
- Bulletin de sécurité de Mandriva du 30 juin 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:109>
- Bulletin de sécurité FreeBSD pour pear-XML_RPC du 03 juillet 2005 :
http://www.vuxml.org/freebsd/pkg-pear-XML_RPC.html
- Bulletin de sécurité Gentoo GLSA 200507-01 du 03 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-01.xml>
- Bulletin de sécurité Gentoo GLSA 200507-02 du 04 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-02.xml>
- Bulletin de sécurité RedHat RHSA-2005:564 du 07 juillet 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-564.html>
- Bulletin de sécurité SUSE SUSE-SA-2005:041 du 08 juillet 2005 :
http://www.novell.com/linux/security/advisories/2005_41_php_pear.html
- Bulletin de sécurité Debian DSA-745 pour drupal du 10 juillet 2005 :
<http://www.debian.org/security/2005/dsa-745>
- Bulletin de sécurité Debian DSA-746 pour phpgroupware du 13 juillet 2005 :
<http://www.debian.org/security/2005/dsa-746>
- Bulletin de sécurité Debian DSA-747 pour egroupeware du 10 juillet 2005 :
<http://www.debian.org/security/2005/dsa-747>
- Bulletin de sécurité Gentoo GLSA 200507-06 pour tikiwiki du 06 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-06.xml>
- Bulletin de sécurité Gentoo GLSA 200507-07 pour phpwebsite du 10 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-07.xml>
- Bulletin de sécurité Gentoo GLSA 200507-08 pour phpgroupware et egroupeware du 10 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-08.xml>
- Bulletin de sécurité OpenBSD pour php4-pear du 12 juillet 2005 :
<http://www.vuxml.org/openbsd/pkg-php4-pear.html>
- Bulletin de sécurité Gentoo GLSA 200507-15 pour php du 15 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-15.xml>
- Bulletin de sécurité SGI 20050703-01-U du 15 juillet 2005 :
<ftp://patches.sgi.com/support/free/security/advisories/20050703-01-U.asc>
- Références CVE CAN-2005-1921 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1921>

Gestion détaillée du document

01 juillet 2005 version initiale.

04 juillet 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200507-01.

04 juillet 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200507-02.

05 juillet 2005 ajout de la référence au bulletin de sécurité FreeBSD.

07 juillet 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200507-06.

11 juillet 2005 ajout des références aux bulletins de sécurité RedHat RHSA-2005:564, SUSE SUSE-SA-2005:041, Debian DSA-745, Debian DSA-747, Gentoo GLSA 200507-06, Gentoo GLSA 200507-07 et Gentoo GLSA 200507-08.

13 juillet 2005 ajout de la référence au bulletin de sécurité OpenBSD.

15 juillet 2005 ajout de la référence au bulletin de sécurité Debian DSA-746.

18 juillet 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200507-15.

18 juillet 2005 ajout de la référence au bulletin de sécurité SGI 20050703-01-U.