



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 août 2005  
N° CERTA-2005-AVI-319-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans PEAR XML\_RPC (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-319>

---

### Gestion du document

Référence	CERTA-2005-AVI-319-001
Titre	Vulnérabilité dans PEAR XML_RPC (PHP)
Date de la première version	23 août 2005
Date de la dernière version	07 octobre 2005
Source(s)	Bulletin de sécurité hardened-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

Exécution de code arbitraire.

## 2 Systèmes affectés

PEAR XML\_RPC versions 1.3.3 et antérieures.

## 3 Résumé

Une vulnérabilité présente dans le module PEAR XML\_RPC permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

## 4 Description

PEAR (PHP Extension and Application Repository) est, comme son nom l'indique, un répertoire de dépôt pour des composants PHP. Le composant XML\_RPC de PEAR est une mise en oeuvre du protocole XML RPC.

Une vulnérabilité présente dans le module PEAR XML\_RPC permet à un utilisateur mal intentionné, via une requête XML RPC malicieusement construite, d'exécuter du code arbitraire PHP sur le système ayant le module vulnérable.

## 5 Solution

La version PEAR XML\_RPC 1.4.0 corrige cette vulnérabilité (cf. section documentation).

## 6 Documentation

- Site Internet de PEAR :  
<http://pear.php.net/>
- Bulletin de sécurité hardened-php :  
[http://www.hardened-php.net/advisory\\_142005.66.html](http://www.hardened-php.net/advisory_142005.66.html)
- Bulletin de sécurité Mandriva MDKSA-2005:146 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:146>
- Bulletin de sécurité Debian DSA-840 pour drupal du 04 octobre 2005 :  
<http://www.debian.org/security/2005/dsa-840>
- Référence CVE CAN-2005-2498 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2498>

## Gestion détaillée du document

**23 août 2005** version initiale.

**07 octobre 2005** ajout de la référence Debian pour drupal.