Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 avril 2007
N° CERTA-2007-AVI-160

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Wordpress

Gestion du document

Référence	CERTA-2007-AVI-160
Titre	Multiples vulnérabilités dans Wordpress
Date de la première version	05 avril 2007
Date de la dernière version	–
Source(s)	Bulletin Wordpress du 03 avril 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

- Atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données ;
- élévation de privilèges.

2 Systèmes affectés

Wordpress versions 2.1.2 et antérieures.

3 Résumé

Plusieurs vulnérabilités de *Wordpress* permettraient de l'exécution de code à distance et une élévation de privilège.

4 Description

Wordpress est une plateforme de publication web écrite en langage PHP.

Une vulnérabilité dans le script `xmlrpc.php` permet à un utilisateur d'élever ses privilèges et de publier même lorsqu'il ne dispose que d'un simple droit de contributeur.

Une vulnérabilité dans l'utilisation du paramètre `post_id` permet de réaliser une injection SQL pouvant porter atteinte à la confidentialité et à l'integrité des données. Cette vulnérabilité n'est exploitable que par un utilisateur authentifié. Un code d'exploitation est disponible sur l'Internet.

5 Solution

Utiliser la version 2.1.3 de *Wordpress*. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin *Wordpress* du 03 avril 2007 :
http://wordpress.org/download/

Gestion détaillée du document

05 avril 2007 version initiale.