



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 janvier 2007
N° CERTA-2007-AVI-034

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Wordpress

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-2007-AVI-034>

Gestion du document

Référence	CERTA-2007-AVI-034
Titre	Vulnérabilité de Wordpress
Date de la première version	17 janvier 2007
Date de la dernière version	–
Source(s)	Bulletin Wordpress du 15 janvier 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 l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Wordpress, versions 2.0.6 et antérieures.

3 Résumé

Wordpress est une plateforme de publication web écrite en langage PHP. Des vulnérabilités permettent des atteintes à la disponibilité et à l'intégrité des données.

4 Description

Les vulnérabilités sont de plusieurs ordres :

- une vulnérabilité dans `wp-admin/templates.php` permet l'injection de scripts ou de code HTML ;

- lorsque le paramétrage PHP active l'option `mbstring`, une personne malintentionnée peut contourner le système de protection des requêtes SQL et ainsi exécuter des commandes SQL arbitraires ;
- les messages d'erreur retournés par `wp-login.php` sont différents selon l'existence ou non de l'utilisateur, ce qui facilite la préparation d'attaques par recherche exhaustive.

5 Solution

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

6 Documentation

- Bulletin de *Wordpress* du 15 janvier 2007 :
<http://wordpress.org/>
- Référence CVE CVE-2006-6808 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6808>
- Référence CVE CVE-2007-0107 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0107>
- Référence CVE CVE-2007-0109 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0109>

Gestion détaillée du document

17 janvier 2007 version initiale.