Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 janvier 2007
N° CERTA-2007-AVI-010

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-010

Gestion du document

Référence	CERTA-2007-AVI-010
Titre	Vulnérabilités dans WordPress
Date de la première version	08 janvier 2007
Date de la dernière version	–
Source(s)	Annonce de la version 2.0.6 de WordPress du 05 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

- Injection de code SQL ;
- contournement de la politique de sécurité.

2 Systèmes affectés

WordPress versions 2.0.5 et antérieures.

3 Description

Deux vulnérabilités ont été découvertes dans *WordPress*.

La première concerne la fonctionnalité de gestion des rétroliens qui ne prend pas en compte correctement tous les encodages de caractères. Cette vulnérabilité requiert l'activation de l'extension `mbstring`. Un utilisateur malintentionné peut exploiter cette vulnérabilité pour injecter du code SQL.

La seconde vulnérabilité a été identifiée dans le système de protection contre les attaques de type `CSRF` (*cross site request forgery*). Un utilisateur malintentionné peut exploiter cette vulnérabilité afin de réaliser une attaque de type *cross site scripting* à l'encontre de l'administrateur, et ainsi exécuter des commandes d'administration ou voler le `cookie` de session.

4 Solution

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

5 Documentation

- Annonce de la version 2.0.6 de WordPress du 05 janvier 2007 :
  http://wordpress.org/development/category/security/
- Téléchargement de la version 2.0.6 de WordPress :
  http://wordpress.org/download/

Gestion détaillée du document

08 janvier 2007 version initiale.