

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-401>

---

### Gestion du document

Référence	CERTA-2007-AVI-401
Titre	Multiples vulnérabilités de Wordpress
Date de la première version	13 septembre 2007
Date de la dernière version	–
Source(s)	Ticket Wordpress 4720
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 indirecte (*cross site scripting*);
- Contournement de la politique de sécurité.

## 2 Systèmes affectés

Wordpress version 2.x et MU 1.x.

## 3 Résumé

Deux vulnérabilités dans *Wordpress* permettent à un utilisateur malveillant de réaliser de l'injection de code indirecte et d'injecter des requêtes SQL.

## 4 Description

Deux vulnérabilités sont présentes dans *Wordpress* :

- un défaut de gestion du filtrage des entrées en HTML permet à un utilisateur malintentionné de poster dans un blog *Wordpress* du code HTML quelconque et des scripts. Ce défaut permet la réalisation d'injection de code indirecte ;

- le filtrage des entrées qui servent à la construction de requêtes SQL est imparfait. Cette vulnérabilité permet à un utilisateur malveillant de modifier les requêtes SQL et de contourner la politique de sécurité.

## **5 Solution**

Les versions 2.2.3 et MU 1.2.5a de *Wordpress* corrigent ces deux problèmes. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## **6 Documentation**

- ticket Wordpress 4720 :  
<http://trac.wordpress.org/ticket/4720>
- Page de téléchargement de Wordpress :  
<http://wordpress.org/download/>

## **Gestion détaillée du document**

**13 septembre 2007** version initiale.