

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-2009-AVI-498>

Gestion du document

Référence	CERTA-2009-AVI-498
Titre	Vulnérabilités dans Wordpress
Date de la première version	13 novembre 2009
Date de la dernière version	–
Source(s)	Mise à jour 2.8.6 de Wordpress du 12 novembre 2009
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

- Contournement de la politique de sécurité ;
- injection de code indirecte.

2 Systèmes affectés

Wordpress versions antérieures à 2.8.6.

3 Résumé

Des vulnérabilités dans Wordpress permettent à une personne malintentionnée d'effectuer une injection de code indirecte et/ou de contourner la politique de sécurité.

4 Description

Deux vulnérabilités ont été corrigées dans Wordpress. La première permet à une personne malintentionnée d'effectuer une attaque de type injection de code indirecte (*cross-site scripting*). La deuxième faille concerne le « nettoyage » des noms de fichiers téléchargés et peut être exploitée dans certaines configurations d'Apache. Les deux vulnérabilités requièrent que l'attaquant se soit authentifié et ait des droits d'écriture.

5 Solution

La version 2.8.6 de Wordpress corrige les problèmes.

6 Documentation

- Annonce de la mise à jour 2.8.6 du 12 novembre 2009 :
<http://wordpress.org/development/2009/11/wordpress-2-8-6-security-release/>

Gestion détaillée du document

13 novembre 2009 version initiale.