

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité 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-334>

---

### Gestion du document

Référence	CERTA-2009-AVI-334-001
Titre	Vulnérabilité dans WordPress
Date de la première version	12 août 2009
Date de la dernière version	19 août 2009
Source(s)	Notes de version 2.8.4 de WordPress du 12 août 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.

## 2 Systèmes affectés

WordPress versions 2.8.3 et antérieures.

## 3 Résumé

Une vulnérabilité dans WordPress permet de réinitialiser, sans les droits requis, un mot de passe à distance.

## 4 Description

Une vulnérabilité a été découverte dans WordPress. Un attaquant peut provoquer la réinitialisation du mot de passe qui correspond au premier compte sans clé dans la base de données (typiquement le compte de l'administrateur). Dans ce cas, un nouveau mot de passe est envoyé par messagerie électronique au propriétaire légitime de ce compte.

## 5 Solution

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

## 6 Documentation

- Notes de version 2.8.4 de WordPress du 12 août 2009 :  
<http://wordpress.org/development/2009/08/2-8-4-security-release/>
- Référence CVE CVE-2009-2762 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2762>

## Gestion détaillée du document

**12 août 2009** version initiale.

**19 août 2009** ajout de la référence CVE.