Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 septembre 2008
N° CERTA-2008-AVI-453-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de WordPress

Gestion du document

Référence	CERTA-2008-AVI-453-001
Titre	Vulnérabilités de WordPress
Date de la première version	10 septembre 2008
Date de la dernière version	19 septembre 2008
Source(s)	Bulletin WordPress du 08 septembre 2008
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, version 2.6.1 et versions précédentes.

3 Résumé

Deux vulnérabilités présentes dans WordPress permettent à un utilisateur malveillant de contourner la politique de sécurité.

4 Description

Une première vulnérabilité affecte la création et la gestion des utilisateurs. Son exploitation permet à un utilisateur malveillant de réinitialiser le mot de passe d'un utilisateur légitime. Le mot de passe de ce dernier est remplacé par un mot de passe créé aléatoirement.

Une deuxième vulnérabilité affecte la fonction PHP *mt_rand*. Dans certaines conditions, la suite pseudoaléatoire produite par cette fonction est prédictible.

Cette fonction est notamment utilisée pour la réinitialisation des mots de passe.

5 Solution

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

6 Documentation

- Site de téléchargement du WordPress :
  http://wordpress.org/
- Bulletin WordPress du 08 septembre 2008 :
  http://wordpress.org/development
- Référence CVE CVE-2008-4106 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4106
- Référence CVE CVE-2008-4107 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4107

Gestion détaillée du document

10 septembre 2008 version initiale.

19 septembre 2008 ajout de références CVE.