Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mai 2011
N° CERTA-2011-AVI-318

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans WordPress

Gestion du document

Référence	CERTA-2011-AVI-318
Titre	Vulnérabilités dans WordPress
Date de la première version	27 mai 2011
Date de la dernière version	–
Source	Annonce de la version 3.1.3 de Wordpress du 25 mai 2011
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 requêtes illégitime par rebond.

2 Systèmes affectés

WordPress versions 3.1.2 et antérieures.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans WordPress 3.1.3 qui permettent à un utilisateur malintentionné de contourner la politique de sécurité ou d'effectuer une attaque de type injection de code indirecte.

4 Description

Plusieurs vulnérabilités ont été corrigées dans WordPress 3.1.3. Elles permettent, notamment, de récupérer la liste des utilisateurs qui ne sont pas des auteurs. Une protection a également été ajoutée dans les pages d'authentification et d'administration afin de se protéger contre des attaques de type injection de requêtes illégitime par rebond (CSRF) en utilisant le champ `'X-Frame-Options'` lorsque le navigateur le supporte.

5 Solution

Mettre WordPress à jour en version 3.1.3.

6 Documentation

- Annonce de la version 3.1.3 de Wordpress du 25 mai 2011 :
  http://wordpress.org/news/2011/05/wordpress-3-1-3/
- Référence CVE CVE-2011-3122 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3122
- Référence CVE CVE-2011-3125 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3125
- Référence CVE CVE-2011-3126 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3126
- Référence CVE CVE-2011-3127 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3127
- Référence CVE CVE-2011-3128 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3128
- Référence CVE CVE-2011-3129 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3129
- Référence CVE CVE-2011-3130 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3130

Gestion détaillée du document

27 mai 2011 version initiale.