

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans WordPress

Gestion du document

Référence	CERTFR-2017-AVI-067
Titre	Multiples vulnérabilités dans WordPress
Date de la première version	07 mars 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité WordPress du 07 mars 2017
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(s)

- contournement de la politique de sécurité
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

WordPress versions antérieures à 4.7.3

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *WordPress*. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, une injection de code indirecte à distance (XSS) et une injection de requêtes illégitimes par rebond (CSRF).

4 - Solution

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

5 - Documentation

- Bulletin de sécurité WordPress du 07 mars 2017
<https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/>

Gestion détaillée du document

07 mars 2017 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-067>
