DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 21-07-2026

BULLETIN ALERTES

Object	Vulnérabilité Critique dans WordPress
Réference	1495
Date de Publication	2026-07-21
Sévérité	Critique

IMPACT :

Compromission complète du serveur web et de la base de données sous-jacente.

Exfiltration de données sensibles, y compris les identifiants administrateur.

DÉSCRIPTION :

Une vulnérabilité critique de type exécution de code à distance (RCE) pré-authentification, surnommée « wp2shell », affecte le noyau de WordPress.

La faille résulte du chaînage de deux vulnérabilités distinctes.

CVE-2026-63030 : confusion de route au niveau du point de terminaison de l'API REST « batch » (/wp-json/batch/v1), exploitable sans authentification ni configuration particulière.

CVE-2026-60137 : injection SQL dans le paramètre author__not_in de la classe WP_Query, permettant notamment la lecture de la base de données, y compris les empreintes de mots de passe administrateur.

Le chaînage de ces deux failles permet à un attaquant anonyme, sans identifiants ni interaction de l'utilisateur, de prendre le contrôle total d'une installation WordPress par défaut, sans qu'aucune extension tierce ne soit requise.

SOLUTION :

Mettre à jour immédiatement vers WordPress 7.0.2 ou 6.9.5 (correctif complet des deux CVE) ; pour la branche 6.8.x, appliquer la version 6.8.6.

DOCUMENTATION :

CVE-2026-63030

cve.org/CVERecord?id=CVE-2026-63030

CVE-2026-60137

cve.org/CVERecord?id=CVE-2026-60137

WordPress.org, « Version 7.0.2 », documentation WordPress, publié le 17 juillet 2026.

wordpress.org/documentation/wordpress-version/version-7-0-2/

Rapid7, « CVE-2026-63030: wp2shell a Critical Remote Code Execution Vulnerability in WordPress Core », Rapid7 Blog, 17 juillet 2026.

rapid7.com/blog/post/etr-cve-2026-63030-wp2shell-a-critical-remote-code-execution-vulnerability-in-wordpress-core/

SecurityWeek, « WP2Shell WordPress Vulnerabilities Exploited in the Wild », 20 juillet 2026.

securityweek.com/wp2shell-wordpress-vulnerabilities-exploited-in-the-wild/

The Hacker News, « New wp2shell WordPress Core Flaw Lets Unauthenticated Attackers Run Code », 18 juillet 2026.

thehackernews.com/2026/07/new-wp2shell-wordpress-core-flaw-lets.html