Boletín de alerta

Boletín Nro.:
Fecha de publicación: 21/07/2026
Tema: Alerta 2026-74 Vulnerabilidad de Ejecución Remota de Código en WordPress
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- WordPress Core 6.9.0 a 6.9.4 (Vulnerable a la cadena completa de RCE)
- WordPress Core 7.0.0 a 7.0.1 (Vulnerable a la cadena completa de RCE)
- WordPress Core 6.8.0 a 6.8.5 (Afectado únicamente por la vulnerabilidad de Inyección SQL)

Descripción

Se ha reportado una nueva cadena de ataque denominada **wp2shell**, la cual permite que un atacante remoto **ejecute código sin necesidad de autenticarse RCE** en sitios que utilizan versiones vulnerables de WordPress. Se identificado dos vulnerabilidades en el core de WordPress: CVE-2026-63030 con un score de 7.5 y CVE-2026-60137 con un score de 9.1.

El ataque combina dos vulnerabilidades:

- **CVE-2026-63030 CVSS 7.5:** Error en el procesamiento por lotes (REST API Batch Routing Confusion).
- **CVE-2026-60137 CVSS 9.1:** Vulnerabilidad de **Inyección SQL** en el núcleo de WordPress.

Al explotarse de forma conjunta, ambas fallas permiten que un atacante envíe una única solicitud HTTP especialmente diseñada para ejecutar código malicioso directamente en el servidor, comprometiendo completamente el sitio web.

La vulnerabilidad afecta incluso a instalaciones estándar de WordPress **sin complementos instalados**, lo que incrementa significativamente el riesgo para organizaciones que ejecutan versiones vulnerables.

Solución:

Se recomienda implementar las siguientes acciones de forma inmediata:

- Actualizar **WordPress 6.9.x** a la versión **6.9.5** o superior.
- Actualizar **WordPress 7.0.x** a la versión **7.0.2** o superior.
- Actualizar la rama **6.8.x** a la versión **6.8.6** para corregir la vulnerabilidad de Inyección SQL.

- Verificar que las actualizaciones automáticas se hayan aplicado correctamente.
- Si la actualización no puede realizarse de inmediato, bloquear temporalmente el acceso a los siguientes endpoints mediante el WAF o firewall:
  - /wp-json/batch/v1
  - ?rest_route=/batch/v1
- Como medida temporal, restringir el acceso anónimo a la API REST hasta completar la actualización.

A continuación le compartimos una guía para actualizar su WordPress:

> **Updating WordPress**

Información adicional:

- **wp2shell: Pre Authentication RCE in WordPress Core › Searchlight Cyber**
- **New wp2shell WordPress Core Flaw Lets Unauthenticated Attackers Run Code**