Nro. Alerta:	AL-2026-038	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	23-jul-2026	Explotación activa de la cadena de vulnerabilidades críticas wp2Shell en WordPress Core	Pág.: **1** of **5**

I. DATOS GENERALES:

Clase de alerta: Explotación activa de vulnerabilidades críticas en WordPress Core (wp2Shell)
Tipo de Incidente: Ejecución remota de código (RCE) mediante cadena de vulnerabilidades en WordPress Core (CVE-2026-60137 y CVE-2026-63030)
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Explotación activa de la cadena de vulnerabilidades críticas wp2Shell en WordPress Core - Figura referencial

La vulnerabilidad wp2Shell corresponde a una cadena de explotación compuesta por dos fallas de seguridad: CVE-2026-63030, asociada a una confusión de rutas (*Path Confusion*) en el mecanismo de procesamiento por lotes (*Batch Processing*) de la API REST y CVE-2026-60137, una inyección SQL presente en el núcleo (*core*) de WordPress. La combinación de ambas fallas permite que un atacante no autenticado comprometa la aplicación y obtenga ejecución remota de código (RCE) en los sistemas afectados. Debido a que el problema reside en el WordPress Core, incluso las instalaciones básicas que no utilizan complementos (*plugins*) ni temas personalizados pueden resultar vulnerables.

III. INTRODUCCIÓN

Varias empresas de ciberseguridad, entre ellas Hexastrike, watchTowr, Cloudflare y Patchstack del propio equipo de seguridad de WordPress, han confirmado la explotación activa de las vulnerabilidades que conforman la cadena wp2Shell. La actividad maliciosa se ha visto facilitada por la disponibilidad pública de pruebas de concepto (*Proof of Concept*, PoC) que demuestran cómo explotar estas fallas. Cabe destacar que ambas vulnerabilidades afectan a diferentes rangos de versiones de WordPress, aspecto que resulta clave para determinar qué sistemas se encuentran expuestos a cada una de ellas.

CVE-2026-60137, corresponde a una falla de inyección SQL (SQL Injection) en el parámetro "author__not_in" de la clase WP_Query, introducida a partir de WordPress 6.8. La vulnerabilidad se origina por una validación insuficiente del tipo de dato recibido, permitiendo que un atacante suministre una cadena de texto en lugar del arreglo esperado. Esta condición posibilita eludir los controles de validación e insertar fragmentos de código SQL arbitrario dentro de las consultas generadas por WordPress, lo que podría derivar en la lectura, modificación o eliminación no autorizada de información almacenada en la base de datos.

CVE-2026-63030 es un fallo lógico en el punto final de la API REST /wp-json/batch/v1 en WordPress 6.9. Este punto final está diseñado para procesar varias sub-solicitudes de la API REST en una única llamada HTTP. Debido a una sincronización incorrecta de los matrices de peticiones internas, un atacante puede crear una petición por lotes en la que una subpetición mal formada provoque que las peticiones posteriores se redirijan a controladores no deseados. Esta confusión permite eludir las listas de permitidos del punto final e inyectar parámetros arbitrarios en llamadas a la API que contienen información confidencial.

La explotación encadenada de ambas fallas permite a un atacante no autenticado inyectar código SQL a través de la API REST, extraer datos confidenciales, como los hashes de contraseñas y en muchos casos, escalar los privilegios hasta lograr la ejecución remota completa de código. Los atacantes pueden subir plugins maliciosos o webshells, modificar el contenido del sitio o aprovechar la brecha para comprometer aún más la infraestructura interna.

IV. VECTOR DE ATAQUE

La vulnerabilidad **CVE-2026-63030** tiene un vector de ataque tipo RED, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N con nivel de severidad 9.8 CRITICA.

La vulnerabilidad **CVE-2026-60137** tiene un vector de ataque tipo RED, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N con nivel de severidad 9.1 CRITICA.

V. IMPACTO

WordPress (desarrollado en PHP), ejecutándose en cualquier sistema operativo compatible con PHP.

Version	Vulnerabilidad
6.8.0 hasta 6.8.5	SQL Injection
6.9.0 hasta 6.9.4	Core (REST API batch route)
7.0.0 hasta 7.0.1	Core (REST API batch route)

Tabla 2.-Versiones afectadas - Explotación activa de la cadena de vulnerabilidades críticas wp2Shell en WordPress Core

VI. INDICADORES DE COMPROMISO

- Archivos PHP creados en las últimas horas.
- Nuevos administradores de WordPress.
- Cambios en plugins o temas.
- Solicitudes repetidas al endpoint /wp-json/batch/v1.
- Parámetros maliciosos en peticiones REST que incluyan author__not_in.
- Actividad SQL anómala en los registros de la base de datos.
- Conexiones salientes inusuales desde el servidor web.

VII. RECOMENDACIONES:

- Actualizar inmediatamente WordPress Core a una versión corregida por el fabricante o aplicar el parche de seguridad correspondiente tan pronto como esté disponible.
- Verificar la versión de WordPress instalada en los servidores y determinar si se encuentra dentro del rango de versiones afectadas.
- Restringir el acceso a la REST API mediante mecanismos de autenticación, listas de control de acceso (ACL) o reglas en el servidor web cuando esta funcionalidad no sea necesaria para la operación del sitio.

- Implementar un Web Application Firewall (WAF) con reglas que permitan detectar y bloquear intentos de explotación dirigidos a la funcionalidad REST API Batch Route.
- Monitorear continuamente los registros del servidor web, PHP y WordPress para identificar solicitudes inusuales hacia la REST API, intentos de ejecución de comandos o actividades sospechosas.
- Revisar periódicamente la integridad de los archivos del sitio web para detectar modificaciones no autorizadas, archivos maliciosos o web shells que puedan indicar una explotación exitosa.
- Aplicar el principio de mínimos privilegios al servicio web y a los procesos que ejecutan PHP, limitando los permisos únicamente a los estrictamente necesarios.
- Mantener copias de seguridad actualizadas y verificadas del sitio web y de la base de datos, con el fin de facilitar la recuperación en caso de compromiso.
- Mantener actualizados el sistema operativo, PHP, el servidor web, los temas y los complementos instalados para reducir la superficie de ataque y minimizar el riesgo de explotación de otras vulnerabilidades.
- Implementar soluciones de monitoreo y detección de amenazas, como SIEM, IDS/IPS o EDR/XDR, que permitan identificar oportunamente actividades anómalas y responder de forma efectiva ante intentos de explotación.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CSIRT TELCONET. (2026). *Vulnerabilidad wp2Shell permite RCE sin autenticación en WordPress Core.*https://csirt.telconet.net/comunicacion/boletines-servicios/vulnerabilidad-wp2shell-permite-rce-sin-autenticacion-en-wordpress-core/

SECURITYWEEK. (2026). *wp2Shell WordPress vulnerabilities exploited in the wild.* https://www.securityweek.com/wp2shell-wordpress-vulnerabilities-exploited-in-the-wild/

Security Boulevard. (2026). *WordPress Remote Code Execution Vulnerability (CVE-2026-63030, CVE-2026-60137) Notice.*https://securityboulevard.com/2026/07/wordpress-remote-code-execution-vulnerability-cve-2026-63030-cve-2026-60137-notice/

RESCANA. (2026). *Active Exploitation Alert: wp2Shell Critical WordPress Core Vulnerabilities (CVE-2026-63030, CVE-2026-60137) Enable Unauthenticated RCE.* https://www.rescana.com/post/active-exploitation-alert-wp2shell-critical-wordpress-core-vulnerabilities-cve-2026-63030-cve-2026-60137-enable-unauthen

HELP NET SECURITY. (2026). *WordPress vulnerabilities: wp2Shell (CVE-2026-63030, CVE-2026-60137).*https://www.helpnetsecurity.com/2026/07/18/wordpress-vulnerabilities-wp2shell-cve-2026-60137-cve-2026-60137/