Boletín de alerta

Boletín Nro.: 108
Fecha de publicación: 23/09/2026
Tema: Alerta 2026-108 Vulnerabilidad Path Traversal y posible RCE en WordPress Core
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Versiones afectadas	Versión corregida
WordPress Core	7.1.0–7.1.1	7.1.2 o superior
WordPress Core	7.0.x	7.0.6 o superior
WordPress Core	6.9.x	6.9.9 o superior
WordPress Core	6.8.x	6.8.10 o superior
WordPress Core	6.7.x	6.7.9 o superior
WordPress Core	6.6.x	6.6.9 o superior
WordPress Core	Ramas anteriores elegibles para correcciones de seguridad, desde 4.7.0	Aplicar el *backport* de seguridad correspondiente; WordPress publicó fixes hasta 4.7.37

Descripción

Se publico una vulnerabilidad etiquetada como **CVE-2026-87902**, la cual es crítica de tipo *path traversal* y carga local de archivos PHP (**Local File Inclusion, LFI**) en WordPress Core. La falla tiene una puntuación **CVSS v4.0 de 9.2** y permite que un atacante remoto no autenticado fuerce a WordPress a incluir un archivo PHP local legible ubicado fuera de los directorios del tema activo. Bajo determinadas condiciones de tema y servidor, el problema puede derivar en **ejecución remota de código (RCE)** y toma completa del sitio.

CVE-2026-87902 es una vulnerabilidad de **control inadecuado de nombres de archivo en operaciones include/require de PHP**, clasificada como **CWE-98**. El problema se encuentra en la lógica con la que

WordPress resuelve el archivo de plantilla de una página, especialmente en las funciones get_page_template() y locate_template().

En versiones vulnerables, una parte de la URL puede utilizarse para construir el nombre de una plantilla con el formato ***page-{valor}.php*** sin validar correctamente secuencias de traversal como ***../***. Un atacante no autenticado puede manipular ese valor para dirigir el proceso de resolución de plantilla hacia un archivo PHP local legible fuera de los directorios permitidos del tema activo.

Solución

La solución definitiva es instalar **WordPress 7.1.2** o el *backport* de seguridad correspondiente a la rama soportada. WordPress no proporciona un *workaround* independiente que elimine la vulnerabilidad.

La actualización puede realizarse mediante:

- **Panel WordPress:** Dashboard > Updates > Update Now.
- **WP‑CLI:** ejecutar la actualización de core siguiendo el procedimiento interno aprobado.
- **Gestores centralizados o plataforma de hosting:** validar que se despliegue la versión corregida y verificar la operación del sitio después de la actualización.

Después de actualizar, confirmar la versión instalada, purgar cachés de WordPress/PHP/CDN/WAF, verificar funcionalidad del tema y realizar un análisis de integridad para descartar actividad previa.

Información adicional:

- https://wordpress.org/news/2026/09/wordpress-7-1-2-release/
- https://www.wordfence.com/blog/2026/09/psa-critical-unauthenticated-path-traversal-vulnerability-patched-in-wordpress-core/
- https://thehackernews.com/2026/09/wordpress-issues-patch-for-critical.html