

Boletín de alerta

Boletín Nro.: 103

Fecha de publicación: 19/09/2026

Tema: Alerta 2026-103 Click2Shell en WordPress permite instalación forzada de temas y puede encadenarse a RCE

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Versiones afectadas	Versión corregida
WordPress Core	WordPress 6.0 hasta versiones previas al parche de seguridad correspondiente	WordPress 7.1.1 o actualización de seguridad equivalente para la rama soportada
WordPress Core — ramas antiguas con soporte de seguridad	Versiones soportadas desde WordPress 4.7 afectadas por el problema	Actualización de mantenimiento/seguridad publicada el 17 de septiembre de 2026

* WordPress confirmó que el problema está presente desde la versión **6.0** hasta las versiones inmediatamente anteriores a la corrección. La actualización de seguridad del 17 de septiembre de 2026 incluye correcciones para ramas soportadas desde WordPress 4.7

Descripción

Se identificó una vulnerabilidad en el núcleo de WordPress que permite que una URL especialmente diseñada fuerce la instalación y previsualización de un tema legítimo desde el repositorio WordPress.org cuando un administrador autenticado abre el enlace. La vulnerabilidad, denominada **Click2Shell**, fue corregida en **WordPress 7.1.1** y en las actualizaciones equivalentes de ramas soportadas. No hay aún un CVE publicado pero se estima un score de 9.6 (crítico).

Click2Shell es una vulnerabilidad de instalación forzada de temas inducida por URL. El problema ocurre porque dos componentes de WordPress interpretan de forma distinta un parámetro incluido en una URL manipulada: el repositorio WordPress.org lo interpreta como el nombre normal de un tema válido, mientras que el navegador del administrador reutiliza el contenido original —incluidos caracteres adicionales— dentro de código JavaScript utilizado para localizar un elemento en la página.

El uso de caracteres especialmente preparados permite que el selector del navegador apunte al botón **Install** y que el propio script de WordPress ejecute la acción de instalación. Como el administrador ya tiene una sesión activa, el navegador incluye automáticamente sus permisos y token de seguridad (*nonce*), por

lo que el atacante no necesita conocer credenciales ni obtener ese token.

Click2Shell no debe confundirse con **wp2shell**, otra vulnerabilidad de WordPress Core divulgada en julio de 2026. wp2shell no requiere inicio de sesión ni interacción de usuario, y CISA la incluyó como vulnerabilidad explotada activamente; Click2Shell, en cambio, requiere que un administrador autenticado abra un enlace especialmente preparado y no tiene explotación activa conocida.

Solución

La solución oficial consiste en actualizar WordPress a **7.1.1** o a la actualización de seguridad publicada para la rama soportada correspondiente. La actualización puede realizarse desde el panel de administración en **Dashboard > Updates > Update Now**, o mediante el paquete de instalación disponible desde WordPress.org.

No existe un *workaround* independiente que elimine el defecto de interpretación de URLs. Deshabilitar temas, restringir el panel administrativo y evitar enlaces sospechosos son controles temporales que reducen la probabilidad de explotación, pero no sustituyen la aplicación del parche.

Tras actualizar, se recomienda mantener únicamente temas y plugins necesarios, aplicar actualizaciones de seguridad con rapidez y usar controles adicionales para proteger las sesiones administrativas.

Información adicional:

- <https://wordpress.org/news/2026/09/wordpress-7-1-1-maintenance-and-security-release/>
- <https://wordpress.org/documentation/wordpress-version/version-7-1-1/>
- <https://thehackernews.com/2026/09/new-wordpress-click2shell-flaw-forces.html>