Boletín de alerta

Boletín Nro.: 85
Fecha de publicación: 07/08/2026
Tema: Alerta 2026-85 XSS Pre-Autenticado con Cadena hacia RCE PHP en WordPress CMS
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

WordPress Core — Sistema de gestión de contenidos (CMS)

Producto	Versiones afectadas	Versión corregida
WordPress	Todas las versiones (desde 4.7 en adelante)	7.0.3
WordPress	Rama 6.9.x	6.9.6
WordPress	Ramas 4.7 – 6.8.x	Backports aplicados

Las versiones anteriores a 4.7 también están afectadas pero quedan fuera del rango de backports oficial del proyecto.

Descripción

Recientemente se ha reportado una vulnerabilidad crítica un XSS reflejado pre-autenticado en la pantalla de login (wp-login.php) en WordPress CMS, etiquetada como CVE-2026-64638 con un score CVSS 8.9 — Alta. Investigadores demostraron que esta falla puede ser encadenada para lograr ejecución remota de código (RCE) en PHP en el servidor cuando un administrador autenticado interactúa con una página controlada por el atacante, convirtiendo un bug del lado del navegador en un compromiso total del servidor.

El problema reside en cómo WordPress procesa el campo username durante intentos de login fallidos. El input pasa por sanitize_user() y wp_strip_all_tags() (que internamente usa strip_tags()), donde una cadena con estructura de etiqueta HTML que incluye un espacio después del < de apertura sobrevive como texto plano. Luego, al pasar por wp_kses_post(), el contenido es interpretado como HTML permitido, generando elementos DOM controlados por el atacante.

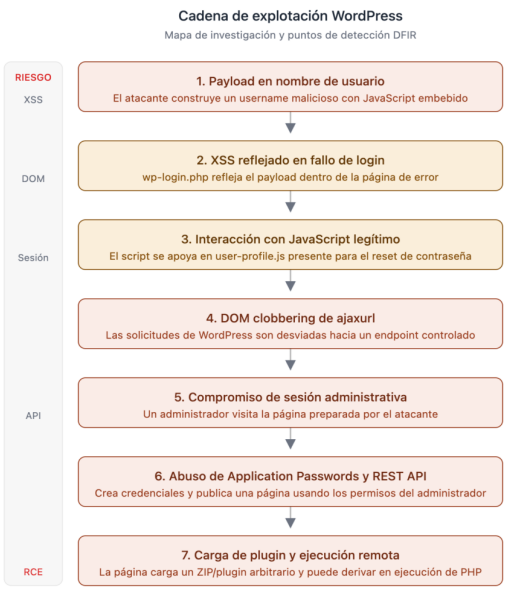

Figura 1 Cadena de Explotación WordPress — CVE-2026-64638: De XSS Pre-Autenticado a Ejecución Remota de Código PHP

Solución

Actualizar de forma inmediata a las versiones corregidas:

Versión actual Actualizar a Método
WordPress 7.0.x 7.0.3 Dashboard Actualizaciones Actualizar ahora
WordPress 6.9.x 6.9.6 Dashboard Actualizaciones Actualizar ahora
WordPress 4.7 – 6.8.x Backport aplicado Actualizaciones automáticas o manual

Descarga oficial:
• https://wordpress.org/download/releases/

Los sitios con actualizaciones automáticas en segundo plano habilitadas ya deberían haber recibido la actualización de seguridad de forma automática. Se recomienda verificar la versión instalada.

Para verificar la instalación puede:

Via WP-CLI

wp core version
wp core update # actualizar si es necesario

Notas de la versión 7.0.3:
• https://wordpress.org/news/2026/08/wordpress-7-0-3-release/

Mitigación

- Implementar un WAF (Web Application Firewall) con reglas de filtrado XSS sobre wp-login.php. Pantheon ya aplicó virtual patching a nivel de red en su plataforma.pantheon

- Restringir el acceso a wp-login.php por IP a través de .htaccess o configuración del servidor web (NGINX/Apache), permitiendo solo IPs conocidas de administradores.
- Deshabilitar la funcionalidad de Application Passwords si no se utiliza, para cortar el vector de la cadena RCE:

add_filter('wp_is_application_passwords_available', '__return_false')

- Monitorear logs de acceso en busca de requests a wp-login.php con usernames que contengan caracteres <, > o similares.

Nota: Los investigadores advirtieron explícitamente que las medidas de hardening estándar de WordPress no deben considerarse mitigación completa para el XSS subyacente. La única solución definitiva es actualizar.

Información adicional:

- The Hacker News — CVE-2026-64638: https://thehackernews.com/2026/08/new-wordpress-pre-auth-xss-could-lead.html
- WordPress 7.0.3 Release (oficial): https://wordpress.org/news/2026/08/wordpress-7-0-3-release/
- WordPress 7.0.3 — Documentación de versión: https://wordpress.org/documentation/wordpress-version/version-7-0-3/
- Security Arsenal — Análisis técnico CVE-2026-64638: https://securityarsenal.com/blog/cve-2026-64638
- Pantheon — Mitigaciones de plataforma: https://docs.pantheon.io/release-notes/2026/08/wordpress-7-0-3
- GitHub Advisory: https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-52p2-r8wf-jcrf