Alert Bulletin

Bulletin N.: 85
Publication Date: 07/08/2026
Subject: Alert 2026-85 Pre-Authenticated XSS with Chain to PHP RCE in WordPress CMS
Traffic Light Protocol (TLP): White

Affected Product(s):

WordPress Core — Content Management System (CMS)

Product	Affected Versions	Fixed Version
WordPress	All versions (from 4.7 onwards)	7.0.3
WordPress	6.9.x branch	6.9.6
WordPress	4.7 – 6.8.x branches	Backports applied

Versions prior to 4.7 are also affected but fall outside the project's official backport range.

Description

A critical pre-authenticated reflected XSS vulnerability has recently been reported on the login screen (wp-login.php) in WordPress CMS, tracked as CVE-2026-64638 with a CVSS score of 8.9 — High. Researchers demonstrated that this flaw can be chained to achieve remote code execution (RCE) in PHP on the server when an authenticated administrator interacts with an attacker-controlled page, turning a browser-side bug into a full server compromise.

The issue lies in how WordPress processes the username field during failed login attempts. The input passes through sanitize_user() and wp_strip_all_tags() (which internally uses strip_tags()), where a string with HTML tag structure that includes a space after the opening < survives as plain text. Then, when passing through wp_kses_post(), the content is interpreted as allowed HTML, generating attacker-controlled DOM elements.

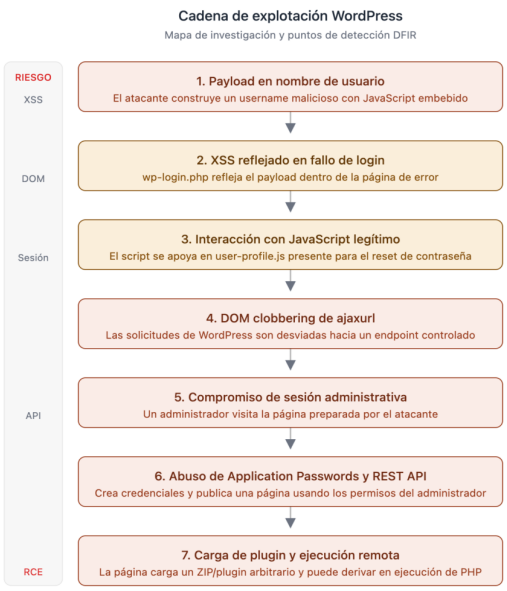

Figure 1 WordPress Exploitation Chain — CVE-2026-64638: From Pre-Authenticated XSS to Remote PHP Code Execution

Solution

Update immediately to the fixed versions:

Current version Update to Method
WordPress 7.0.x 7.0.3 Dashboard Updates Update now
WordPress 6.9.x 6.9.6 Dashboard Updates Update now
WordPress 4.7 – 6.8.x Backport applied Automatic or manual updates

Official download:
• https://wordpress.org/download/releases/

Sites with automatic background updates enabled should have already received the security update automatically. It is recommended to verify the installed version.

To verify the installation you can:

Via WP-CLI

wp core version
wp core update # update if necessary

Version 7.0.3 release notes:
• https://wordpress.org/news/2026/08/wordpress-7-0-3-release/

Mitigation

- Implement a WAF (Web Application Firewall) with XSS filtering rules on wp-login.php. Pantheon has already applied virtual patching at the network level on its platform.pantheon

- Restrict access to wp-login.php by IP through .htaccess or web server configuration (NGINX/Apache), allowing only known administrator IPs.
- Disable the Application Passwords functionality if not used, in order to cut the RCE chain vector:

add_filter('wp_is_application_passwords_available', '__return_false')

- Monitor access logs for requests to wp-login.php with usernames containing characters such as or similar.

Note: Researchers explicitly warned that standard WordPress hardening measures should not be considered complete mitigation for the underlying XSS. The only definitive solution is to update.

Additional information:

- The Hacker News — CVE-2026-64638: https://thehackernews.com/2026/08/new-wordpress-pre-auth-xss-could-lead.html
- WordPress 7.0.3 Release (official): https://wordpress.org/news/2026/08/wordpress-7-0-3-release/
- WordPress 7.0.3 — Version documentation: https://wordpress.org/documentation/wordpress-version/version-7-0-3/
- Security Arsenal — Technical analysis CVE-2026-64638: https://securityarsenal.com/blog/cve-2026-64638
- Pantheon — Platform mitigations: 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