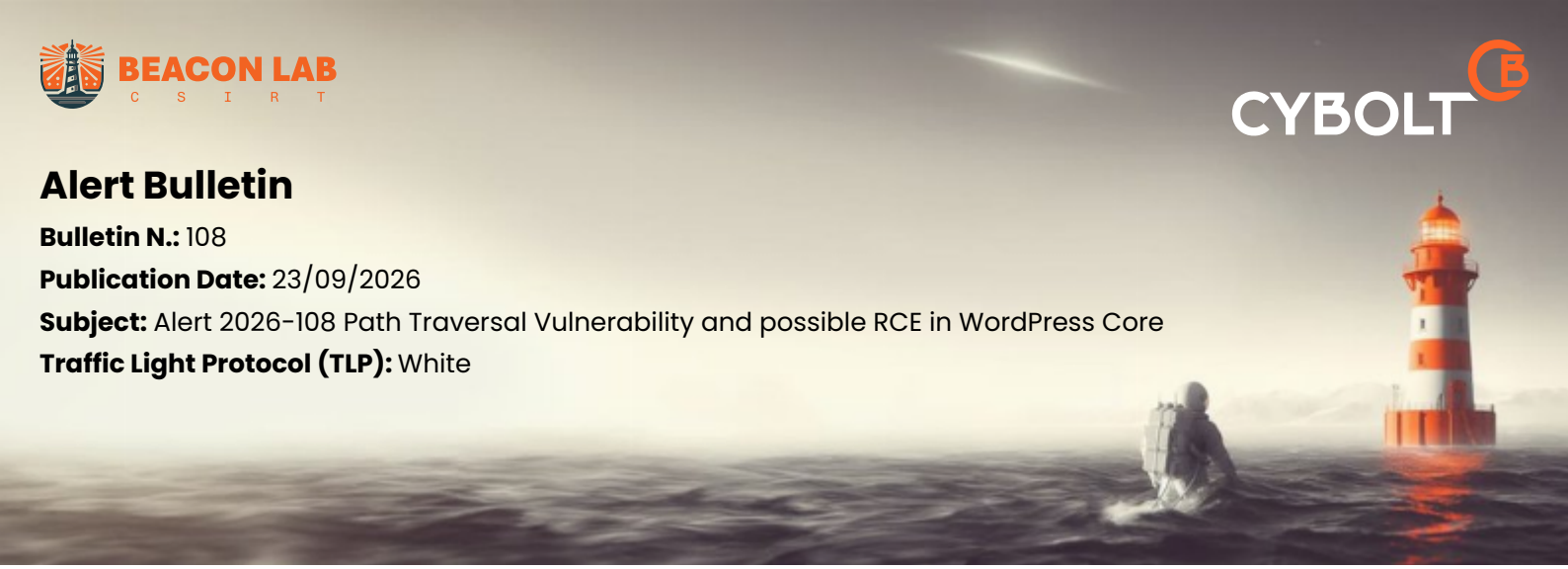

Alert Bulletin

Bulletin N.: 108
Publication Date: 23/09/2026
Subject: Alert 2026-108 Path Traversal Vulnerability and possible RCE in WordPress Core
Traffic Light Protocol (TLP): White

Affected product(s):

Product	Affected versions	Fixed version
WordPress Core	7.1.0–7.1.1	7.1.2 or higher
WordPress Core	7.0.x	7.0.6 or higher
WordPress Core	6.9.x	6.9.9 or higher
WordPress Core	6.8.x	6.8.10 or higher
WordPress Core	6.7.x	6.7.9 or higher
WordPress Core	6.6.x	6.6.9 or higher
WordPress Core	Previous branches eligible for security fixes, since 4.7.0	Apply the corresponding security *backport*; WordPress published fixes up to 4.7.37

Description

A vulnerability labeled **CVE-2026-87902** was published, which is critical of *path traversal* type and local PHP file loading (**Local File Inclusion, LFI**) in WordPress Core. The flaw has a **CVSS v4.0 score of 9.2** and allows an unauthenticated remote attacker to force WordPress to include a readable local PHP file located outside the active theme directories. Under certain theme and server conditions, the issue can lead to **remote code execution (RCE)** and full site takeover.

CVE-2026-87902 is a vulnerability of **inadequate control of file names in PHP include/require operations**, classified as **CWE-98**. The issue lies in the logic with which WordPress resolves the template file of a page, especially in the get_page_template() and locate_template() functions.

In vulnerable versions, a part of the URL can be used to construct the name of a template in the format ***page-{value}.php*** without correctly validating traversal sequences such as **../**. An unauthenticated attacker can manipulate that value to direct the template resolution process toward a readable local PHP file outside the allowed directories of the active theme.

Solution

The definitive solution is to install **WordPress 7.1.2** or the corresponding security *backport* for the supported branch. WordPress does not provide an independent *workaround* that eliminates the vulnerability.

The update can be performed via:

- **WordPress Dashboard:** Dashboard > Updates > Update Now.
- **WP CLI:** run the core update following the approved internal procedure.
- **Centralized managers or hosting platform:** validate that the fixed version is deployed and verify the site's operation after the update.

After updating, confirm the installed version, purge WordPress/PHP/CDN/WAF caches, verify theme functionality, and perform an integrity analysis to rule out prior activity.

Additional information:

- 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