Critical vulnerability in WordPress Core

This is an urgent security advisory regarding a critical security vulnerability related to WordPress Core. Immediate action is required to ensure affected services are patched immediately.

Summary of Critical Vulnerability

- **Vulnerability Name:** wp2shell (REST API route-confusion - CVE-2026-63030 and SQL injection flaw - CVE-2026-60137)
- **Severity:** Critical (CVSS 10.0)
- **Type:** Remote Code Execution (RCE) vulnerability due to route confusion and SQL injection primitives in the WordPress REST batch endpoint used to handle bundled sub-requests.
- **Status:** Actively exploited in the wild and monitored by global security labs with automated proof-of-concept (PoC) tools publicly circulating on GitHub.
- **Impact:** Unauthenticated remote attackers can execute arbitrary code and completely compromise affected servers. This requires no credentials, plugins, or user interaction.
- **Affected Frameworks and Bundles:**
    - WordPress Core installations running branches 6.9.0 to 6.9.4 and 7.0.0 to 7.0.1
    - SQL injection exposure on branches 6.8.0 to 6.8.5

Recommendations for urgent action

- All services utilizing WordPress Core and dependent plugins must immediately apply the recommended patches to prevent unauthenticated Remote Code Execution (RCE).
- Update WordPress core installations need t to the latest patched versions: 6.8.6, 6.9.5 and 7.0.2

Note that due to downstream dependencies, it is critical to refer to the official vendor's advisory and the affected host's documentation to confirm the required versions and updates.

References:

1. https://www.elastic.co/security-labs/wp2shell-wordpress-rce-detection-elastic-defend
2. https://wordpress.org/news/2026/07/wordpress-7-0-2-release/