GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

22 July 2026

Advisory 171: WordPress Core REST API Batch-Route Confusion ("wp2shell") Vulnerability

Release Date: 21st July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate WordPress-based websites, including gov.vu sites and partner organizations. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-63030 is a REST API batch-route confusion vulnerability in WordPress Core, publicly referred to as "wp2shell," that allows an unauthenticated attacker to reach code paths that should require authentication.

On its own, the weakness is bounded. Its severity comes from its ability to unlock a second, more serious flaw - CVE-2026-60137.

What are the systems affected?

No account or user interaction is required - per the GitHub Security Advisory and multiple vendor analyses, this vulnerability is exploitable by unauthenticated attackers against a stock WordPress installation with no plugins.

WordPress Core 6.9.0 through 6.9.4 - Affected (full RCE chain)

WordPress Core 7.0.0 through 7.0.1 - Affected (full RCE chain)

WordPress Core 6.8.0 through 6.8.5 - Affected (companion SQL injection CVE-2026-60137 only)

WordPress Core 6.9.5 and 7.0.2 - Patched

What does this mean?

Both vulnerabilities are remotely exploitable with low attack complexity. Once chained, they allow full compromise of the site and its underlying database.

Step 1 - Route Confusion / Auth Bypass
The attacker sends a specially crafted request to the WordPress REST API batch endpoint (/wp-json/batch/v1), exploiting the route confusion to bypass authentication that would normally gate certain internal routes.

Step 2 - SQL Injection
The now-reachable code path is used to trigger the SQL injection in WP_Query's author_not_in parameter, allowing the attacker to manipulate database queries.

Step 3 - Remote Code Execution
The SQL injection is leveraged to achieve remote code execution on the underlying server, giving the attacker full control of the site and its data.

Step 4 - Persistence
Observed campaigns have deployed persistent webshells and installed malicious plugins to maintain access after initial compromise - no user interaction, credentials, or plugins are required at any stage.

Mitigation process

CERTVU recommends the following:

Update WordPress 7.0.0 or 7.0.1 to 7.0.2 or later.

Update WordPress 6.9.0 through 6.9.4 to 6.9.5 or later.

Update WordPress 6.8.0 through 6.8.5 to 6.8.6 or later to close the companion SQL injection.

Verify the update has actually applied - WordPress has enabled forced automatic updates for affected installations, but administrators should confirm rather than assume.

Inventory all WordPress instances across gov.vu infrastructure and partner sites as a priority, given the scale of WordPress's installed base.

No official workaround is recommended at this time - patching is the only effective remediation.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-63030
2. https://www.rapid7.com/blog/post/etr-cve-2026-63030-wp2shell-a-critical-remote-code-execution-vulnerability-in-wordpress-core/
3. https://www.vulncheck.com/blog/wp2shell
4. https://www.cycognito.com/blog/emerging-threat-cve-2026-63030-cve-2026-60137-wordpress-core-unauthenticated-rce-via-wp2shell/
5. https://kevintel.com/CVE-2026-63030