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 172: WordPress Core SQL Injection Vulnerability_CVE-2026-60137

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-2026-60137 is a SQL injection vulnerability in the author__not_in parameter of WP_Query, the core WordPress class responsible for building most of the database queries WordPress issues. It is classified as CWE-89 and carries a CVSS v3.1 base score of 9.1 (Critical) on its own.

This vulnerability is the companion flaw referenced in CERTVU Advisory 171 (CVE-2026-63030, the "wp2shell" REST API batch-route confusion issue). On WordPress 6.9 and higher, this SQL injection combines with CVE-2026-63030 to reach full unauthenticated remote code execution, publicly tracked as the "wp2shell" attack chain. On the 6.8.x branch, WordPress states this SQL injection is independently exploitable even though that branch is not listed as vulnerable to the full RCE chain.

What are the systems affected?

No account or user interaction is required to trigger this vulnerability once the relevant code path is reached; on WordPress 6.9 and above this requires the route-confusion bypass described in Advisory 171, while on 6.8.x it can be reached directly.

WordPress Core 6.8.0 through 6.8.5 – Affected (SQL injection, independently exploitable)

WordPress Core 6.9.0 through 6.9.4 – Affected (SQL injection; combines with CVE-2026-63030 for full RCE)

WordPress Core 7.0.0 through 7.0.1 – Affected (SQL injection; combines with CVE-2026-63030 for full RCE)

WordPress Core 6.8.6, 6.9.5, and 7.0.2 – Patched

What does this mean?

This vulnerability is remotely exploitable with low attack complexity. Its impact depends on the branch: on 6.8.x it allows direct SQL injection against the WordPress database; on 6.9.x and 7.0.x it is the second stage of the full "wp2shell" remote code execution chain.

Step 1 - Reaching the Vulnerable Query
On WordPress 6.9 and above, the attacker first uses the REST API batch-route confusion issue (CVE-2026-63030, see Advisory 171) to reach an internal code path without authentication. On WordPress 6.8.x, this parameter may be reachable without that additional step.

Step 2 - SQL Injection via author__not_in
The attacker supplies a crafted value for the author__not_in parameter processed by WP_Query, which is insufficiently sanitized, allowing injected SQL to be executed against the WordPress database.

Step 3 - Data Access or Escalation to Code Execution
On its own, the injection can expose or manipulate database contents. When chained with CVE-2026-63030 on WordPress 6.9 and above, it is leveraged further to achieve remote code execution on the underlying server.

Step 4 - Persistence
Observed campaigns exploiting the full chain have deployed persistent webshells and installed malicious plugins to maintain access after initial compromise.

Mitigation process

CERTVU recommends the following:

Update WordPress 6.8.0 through 6.8.5 to 6.8.6 or later.

Update WordPress 6.9.0 through 6.9.4 to 6.9.5 or later.

Update WordPress 7.0.0 or 7.0.1 to 7.0.2 or later.

Treat this patch as equally urgent on the 6.8.x branch, even though that branch is not affected by the full RCE chain — the standalone SQL injection is independently rated 9.1 (Critical).

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

Review Advisory 171 (CVE-2026-63030) alongside this advisory, since the two vulnerabilities are commonly remediated together via the same WordPress Core update.

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

Reference

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