An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2607200218

NCSC Advisory

Multiple Vulnerabilities in WordPress Core: CVE-2026-63030 and CVE-2026-60137

20th, July 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-63030

Published: 2026-07-17

Vendor: WordPress

Product: WordPress

CVSS Score[1]: 7.5

Products Affected

Product	Version
WordPress	6.9.0 < 6.9.5
WordPress	7.0.0 < 7.0.2

Impact

WordPress versions 6.9 and higher are vulnerable to a REST API batch-route confusion weakness. WordPress 6.9.x before 6.9.5 and 7.0.x before 7.0.2 is affected by a REST API batch endpoint route confusion issue which, combined with the author_not_in WP_Query SQL Injection (CVE-2026-60137), could allow an attacker to perform SQL Injection and achieve Remote Code Execution.

Common Weakness Enumeration (CWE)[2]: CWE-436: Interpretation Conflict

CISA Known Exploited Vulnerability (KEV) catalog[3]: No

KevIntel Known Exploited Vulnerability (KEV) catalog[4]: Yes

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[4] https://kevintel.com/feed

Description

CVE ID: CVE-2026-60137

Published: 2026-07-17

Vendor: WordPress

Product: WordPress

CVSS Score: 9.1

Products Affected

Product	Version
WordPress	6.8.0 < 6.8.6
WordPress	6.9.0 < 6.9.5
WordPress	7.0.0 < 7.0.2

Impact

WordPress versions 6.8 and higher are vulnerable to an SQL Injection issue. WordPress 6.8.x before 6.8.6, 6.9.x before 6.9.5, and 7.0.x before 7.0.2 does not properly sanitise the author_not_in parameter of WP_Query, which could allow SQL Injection when a plugin or theme passes untrusted input to the parameter.

Common Weakness Enumeration (CWE): CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CISA Known Exploited Vulnerability (KEV) catalog: No

KevIntel Known Exploited Vulnerability (KEV) catalog: Yes

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from WordPress.

CVE-2026-63030

- https://nvd.nist.gov/vuln/detail/CVE-2026-63030
- https://www.cve.org/CVERecord?id=CVE-2026-63030
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-ff9f-jf42-662q
- https://wordpress.org/news/2026/07/wordpress-7-0-2-release/
- https://wp2shell.com/

CVE-2026-60137

- https://nvd.nist.gov/vuln/detail/CVE-2026-60137
- https://www.cve.org/CVERecord?id=CVE-2026-60137
- https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-fpp7-x2x2-2mjf
- https://wordpress.org/news/2026/07/wordpress-7-0-2-release/
- https://wp2shell.com/