An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611270228

NCSC Advisory

Vulnerabilities in WordPress Foundation: WordPress

CVE-2026-119977

27 November 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-2026-119977

Published: 2026-10-31

Vendor: WordPress Foundation

Product: WordPress

CVSS Score[1]: 8.1

Products Affected

Product	Version
WordPress	4.7.0 <= 4.7.38
WordPress	4.8.0 <= 4.8.33
WordPress	4.9.0 <= 4.9.34
WordPress	5.0.0 <= 5.0.30
WordPress	5.1.0 <= 5.1.27
WordPress	5.2.0 <= 5.2.29
WordPress	5.3.0 <= 5.3.26
WordPress	5.4.0 <= 5.4.24
WordPress	5.5.0 <= 5.5.23
WordPress	5.6.0 <= 5.6.22
WordPress	5.7.0 <= 5.7.20
WordPress	5.8.0 <= 5.8.18
WordPress	5.9.0 <= 5.9.19
WordPress	6.0.0 <= 6.0.17
WordPress	6.1.0 <= 6.1.15
WordPress	6.2.0 <= 6.2.14
WordPress	6.3.0 <= 6.3.13

[1] https://www.first.org/cvss/

WordPress	6.4.0 <= 6.4.13
WordPress	6.5.0 <= 6.5.13
WordPress	6.6.0 <= 6.6.10
WordPress	6.7.0 <= 6.7.10
WordPress	6.8.0 <= 6.8.11
WordPress	6.9.0 <= 6.9.10
WordPress	7.0.0 <= 7.0.7
WordPress	7.1.0 <= 7.1.3

Impact

WordPress Core is vulnerable to Remote Code Execution in versions 4.7 through 7.1.3. This is due to predictable, web-accessible staging paths used during full-package core upgrades. This makes it possible for unauthenticated attackers to execute code on the server during the upgrade window.,

Common Weakness Enumeration (CWE)[2]: CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

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 Foundation.

- https://nvd.nist.gov/vuln/detail/CVE-2026-119977
- https://www.cve.org/CVERecord?id=CVE-2026-119977
- https://www.wordfence.com/threat-intel/vulnerabilities/id/4b4da0cf-d9f4-47c4-a0e8-6c4dc5a6f250?source=cve
- https://wordpress.org/news/2026/10/wordpress-7-1-4/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-119977