CISA Adds WordPress Core Race-Condition Flaw to Known Exploited Vulnerabilities Catalog



CISA has added CVE-2026-119977, a high-severity WordPress Core flaw, to its KEV catalog on evidence of active exploitation. The race-condition issue could allow arbitrary code execution.

- CISA added a WordPress Core vulnerability to its Known Exploited Vulnerabilities (KEV) catalog.
- The flaw is tracked as CVE-2026-119977 with a CVSS score of 8.1, rated high severity.
- It is a Time-of-check Time-of-use (TOCTOU) race condition.
- The flaw could be exploited to achieve arbitrary code execution.
- CISA cites evidence of active exploitation.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a flaw in WordPress Core to its

Known Exploited Vulnerabilities (KEV) catalog, saying there is evidence it is being exploited in the wild.

What is known

The vulnerability is tracked as **CVE-2026-119977** and carries a CVSS score of 8.1, which places it in the high-severity range. It is a Time-of-check Time-of-use (TOCTOU) race condition. According to the report, it could be exploited to achieve arbitrary code execution.

The source report is brief and, in the portion available to us, does not describe affected versions, patched releases, the exact conditions needed for exploitation, or who is behind the attacks. Readers should therefore treat the vendor's official security advisory as the authoritative reference for those details.

Why it matters

Inclusion in the KEV catalog signals that exploitation is not theoretical. For institutions that run WordPress for public websites, customer portals or investor and media pages, a code-execution flaw in the core platform can expose the hosting environment and any data reachable from it.

Recommended approach

Organisations should first establish where WordPress is in use, including sites managed by marketing teams or third-party agencies. They should then consult the official WordPress security guidance for the fixed version and schedule the update through normal change control, prioritising internet-facing sites. Monitoring for unusual file changes or unexpected administrative activity is a sensible precaution while patching is under way.

What to do now

1. Inventory all WordPress instances, including those run by agencies or business units.
2. Check the official WordPress security advisory for CVE-2026-119977 and identify the fixed version.
3. Patch internet-facing WordPress sites first, through change control.
4. Review web server and WordPress logs for unexpected file changes or administrative activity.
5. Add CVE-2026-119977 to vulnerability tracking with a remediation deadline.