CVE-2026-119977

WordPress WordPress Core Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability

CISA KEV since Nov 3, 2026 | Actively exploited

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.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	8.1	0.006	Nov 6, 2026
Urgent priority	High · NVD	48.8th percentile · FIRST	CISA federal deadline in 2 days

Signals behind the score

counted in the score | not counted — evidence for 6 of 8 signals

☑ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☑ KEV recency	Added to CISA KEV within the last 30 days
☑ EPSS	0.006 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☑ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle — Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
WordPress / WordPress Core	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-p6jj-qrp3-7m4g	**wordpress.org**	wordpress.org/news/2026/10/wordpress-7-1-4
wordfence.com	wordfence.com/threat-intel/vulnerabilities/wordpress-core/wordpress-core-470-713-unauthenticated-upgrade-window-staged-installer-remote-code-execution	**BOD 26-04**	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	**NVD**	nvd.nist.gov/vuln/detail/CVE-2026-119977
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	**ENISA EUVD**	euvd.enisa.europa.eu/vulnerability/EUVD-2026-114575
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-119977		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.