

Remote Code Execution Vulnerability Found within WordPress Core During Full-Package Upgrades

High Attack Complexity	Upgrade Window Only	Active Exploitation	Updates Available

The Cal-CSIC has become aware of a remote code execution vulnerability, CVE-2026-119977, affecting WordPress Core versions 4.7 through 7.1.3. WordPress is a content management system used to build and administer websites, and a successful attack could allow an unauthenticated attacker to run code on the server hosting an affected site. The vulnerability carries a CVSS 3.1 score of 8.1 in its CVE record.[1, 2] WordPress rates the issue Low in its own advisory.[3]

The vulnerability is a time-of-check to time-of-use (TOCTOU) race condition in the WordPress Core update process, not in a plugin or theme.[1] During a full-package core update, affected versions extract the update into a predictable directory under wp-content/upgrade, which a web server may serve directly, and the staged copy includes the WordPress installer file wp-admin/setup-config.php.[1, 4] A successful exploit could allow the attacker to execute arbitrary PHP code on the server by requesting the staged file directly before it is removed. No credentials or user interaction are required, but attack complexity is high: the attacker must request the file during a staging window that open-source reporting indicates typically lasts only seconds, and the web server must serve and execute PHP from the staging directory.[1, 4]

WordPress released version 7.1.4 on October 28, 2026, with security fixes backported to every branch back to 4.7; the fixed release for each branch is listed below.[5] Branches 4.6 and earlier received no fix.[4] Open-source reporting has documented exploitation attempts beginning shortly after the release, including more than 18,500 requests against staged installer paths in the first 21 hours, but had not documented a confirmed compromise as of October 31, 2026.[4] CISA added CVE-2026-119977 to its Known Exploited Vulnerabilities (KEV) catalog on November 3, 2026, based on evidence of active exploitation.[6] As of November 5, 2026, the open-source reporting reviewed by the Cal-CSIC did not document a publicly available proof-of-concept (PoC) exploit, which does not establish that none exists.[4, 7] The official fix is the only permanent resolution; restricting direct web access to wp-content/upgrade is a temporary defense-in-depth measure until patching is complete.[7]

The Cal-CSIC recommends that clients running self-managed WordPress installations promptly update WordPress Core to the fixed release for their specific branch, prioritize internet-facing sites, and confirm that background automatic updates have applied successfully. When feasible, clients are advised to perform manual core upgrades during planned maintenance windows with temporary web access restrictions placed on wp-admin and wp-content/upgrade. Following the update, administrators should verify the core version and file

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

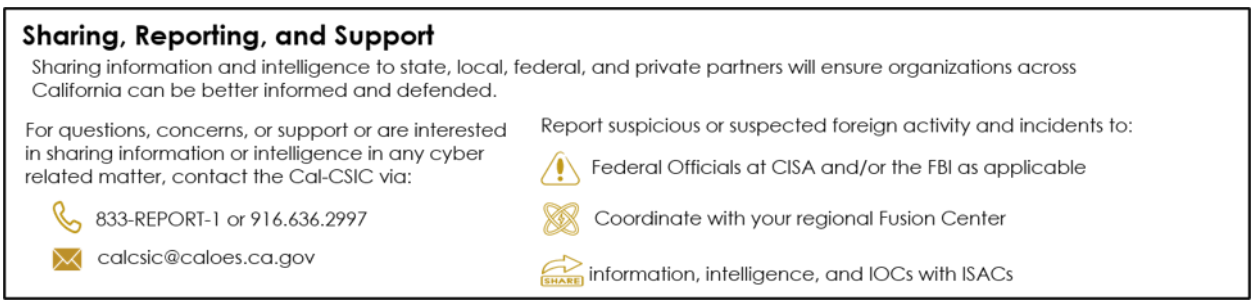
integrity (e.g., using wp core version and wp core verify-checksums), inspect web server logs for requests targeting wp-content/upgrade during update windows on or after October 28, 2026, and review installation directories for unauthorized PHP files, unfamiliar administrator accounts, and unauthorized plugins. Clients on WordPress 4.6 or earlier should upgrade to a supported release.

Affected Products and Versions

Product	Affected Version	Fixed Release		Product	Affected Version	Fixed Release
WordPress Core 7.1	7.1.0–7.1.3	7.1.4		WordPress Core 5.8	5.8.0–5.8.18	5.8.19
WordPress Core 7.0	7.0.0–7.0.7	7.0.8		WordPress Core 5.7	5.7.0–5.7.20	5.7.21
WordPress Core 6.9	6.9.0–6.9.10	6.9.11		WordPress Core 5.6	5.6.0–5.6.22	5.6.23
WordPress Core 6.8	6.8.0–6.8.11	6.8.12		WordPress Core 5.5	5.5.0–5.5.23	5.5.24
WordPress Core 6.7	6.7.0–6.7.10	6.7.11		WordPress Core 5.4	5.4.0–5.4.24	5.4.25
WordPress Core 6.6	6.6.0–6.6.10	6.6.11		WordPress Core 5.3	5.3.0–5.3.26	5.3.27
WordPress Core 6.5	6.5.0–6.5.13	6.5.14		WordPress Core 5.2	5.2.0–5.2.29	5.2.30
WordPress Core 6.4	6.4.0–6.4.13	6.4.14		WordPress Core 5.1	5.1.0–5.1.27	5.1.28
WordPress Core 6.3	6.3.0–6.3.13	6.3.14		WordPress Core 5.0	5.0.0–5.0.30	5.0.31
WordPress Core 6.2	6.2.0–6.2.14	6.2.15		WordPress Core 4.9	4.9.0–4.9.34	4.9.35
WordPress Core 6.1	6.1.0–6.1.15	6.1.16		WordPress Core 4.8	4.8.0–4.8.33	4.8.34
WordPress Core 6.0	6.0.0–6.0.17	6.0.18		WordPress Core 4.7	4.7.0–4.7.38	4.7.39
WordPress Core 5.9	5.9.0–5.9.19	5.9.20				

Affected versions are all releases from the listed base release through the release immediately before the fixed release. WordPress 4.6 and earlier receive no security updates; clients on those versions should upgrade to a supported release.

Sharing, Reporting, and Support



WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

References

[1] Wordfence; "WordPress Core 4.7.0 - 7.1.3: Unauthenticated Upgrade-Window Staged Installer Remote Code Execution"; https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-core/wordpress-core-470-713-unauthenticated-upgrade-window-staged-installer-remote-code-execution?asset_slug=wordpress; Accessed November 5, 2026.
[2] NIST National Vulnerability Database; "CVE-2026-119977 Detail"; https://nvd.nist.gov/vuln/detail/cve-2026-119977; Accessed November 5, 2026.
[3] WordPress; "GHSA-4w3m-c66w-69mg"; https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-4w3m-c66w-69mg; October 29, 2026.
[4] Brandefense; "WordPress 7.1.4 Security Update"; https://brandefense.io/security-news/wordpress-7-1-4-security-update-upgrade-window/; Accessed November 5, 2026.
[5] WordPress.org; "WordPress 7.1.4 Security Release"; https://wordpress.org/news/2026/10/wordpress-7-1-4/; October 28, 2026.
[6] CISA; "Known Exploited Vulnerabilities Catalog: CVE-2026-119977"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-119977; November 3, 2026; Accessed November 5, 2026.
[7] SOC Prime; "CVE-2026-119977: WordPress Core RCE Exploited"; https://socprime.com/blog/cve-2026-119977-wordpress-core-rce-flaw-exploited-during-software-upgrades/; Accessed November 5, 2026.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.