Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

WordPress Core RCE Exploited in the Upgrade Window

Date of Publication	Admiralty Code	TA Number
November 05, 2026	A1	TA2026323

Summary

First Seen: October 28, 2026
Affected Products: WordPress Core
Impact: CVE-2026-119977 is a high-severity remote code execution flaw in WordPress Core that opens a brief gap during full core updates. While WordPress unpacks a new release, it stages the complete package, including the installer, in a predictable folder under wp-content/upgrade that is often reachable from the web. An unauthenticated attacker who requests the staged installer at the right moment can interact with that half-installed copy and achieve PHP code execution on the server. WordPress fixed the flaw in version 7.1.4 on October 28, 2026, but attackers moved fast: Wordfence blocked 62,969 attempts in a single 24-hour period. No threat actor or malware family has been publicly attributed to the activity.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-119977	WordPress WordPress Core Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability	WordPress Core	✗	✓	✓

Vulnerability Details

#1

CVE-2026-119977 is a time-of-check to time-of-use (TOCTOU) race condition in WordPress Core, classified under CWE-367, that leads to unauthenticated remote code execution. The flaw does not sit in a plugin or a theme but in the core upgrade routine itself, which is what makes it relevant to such a wide installed base.

#2

The root cause is the way WordPress stages a full-package core update. When a site installs a complete core release rather than a smaller incremental patch, WordPress unpacks the new files into a predictable directory under wp-content/upgrade before moving them into place. That unpacked copy includes the WordPress installer files. On many hosting setups, the staging directory is served over the web, and PHP will execute from it, which means a complete, writable, installable copy of WordPress briefly exists at a path an outsider can guess or discover. An unauthenticated attacker who requests the installer at precisely the right moment can interact with the staged WordPress copy and progress to PHP code execution.

#3

Exploitation is a race, and winning it requires several conditions to line up at once: the update must be a full-package one that contains the installer files, the staging tree must be reachable over the web with PHP execution enabled, the staging path must be predictable or discoverable, and the attacker must finish before WordPress cleans up the temporary files. The attack requires hitting a very narrow window while WordPress is unpacking a complete core update, and in normal lab conditions that window lasts only seconds. All versions from WordPress 4.7 through 7.1.3 are affected, and the fix landed in WordPress 7.1.4 on October 28, 2026.

#4

Active exploitation began almost immediately after the patch was published, which strongly suggests attackers worked back from the fix. Rather than wait for a lucky moment, they are polling vulnerable paths such as setup-config.php over and over in the hope of catching a site mid-upgrade. Wordfence blocked 62,969 attacks in the 24 hours it reported on October 30, 2026, and 13,095 more in a 24-hour span the following weekend. Two of the largest sources repeatedly polled small groups of sites for around 14.5 hours, behavior described as consistent with trying to catch the brief upgrade window, while other sources tested many staging-directory and version-name variations.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-119977	WordPress WordPress Core (versions 4.7 through 7.1.3)	cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*	CWE-367

Recommendations

Update to WordPress 7.1.4 Right Away: Move every site to WordPress 7.1.4 without delay. This is the only fix for the flaw, and because exploitation attempts are already running at scale, every hour a site stays on 4.7.0 through 7.1.3 is an hour it can be caught mid-upgrade. If you manage many sites, patch the internet-facing and high-value ones first rather than working through a list alphabetically.

Check Whether You Were Hit During a Recent Update: Go back through your web server logs and look for requests to PHP files under wp-content/upgrade, especially installer files such as setup-config.php, around the times your sites ran core updates. Repeated requests to staging paths from the same source, or probes that walk through different version-name and directory variations, are the clearest sign that someone was waiting for your upgrade window.

Hunt for What an Attacker Would Leave Behind: If code execution succeeded, the attacker needed somewhere to persist. Review your WordPress dashboard for administrator accounts you do not recognize, plugins nobody on your team installed, and PHP files that do not belong in the directories they are sitting in. Anything unfamiliar should be removed, and you should reset passwords for the accounts you trust and rotate any secrets stored on the server.

Close Off the Staging Directory: The attack only works because the upgrade folder is reachable from the web and will execute PHP. Configure your web server to deny direct requests to wp-content/upgrade and to block PHP execution inside it. This does not replace the patch, but it removes the condition the whole technique depends on and protects you against similar staging-path issues in the future.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	

Patch Link

https://wordpress.org/download/

References

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-core/wordpress-core-470-713-unauthenticated-upgrade-window-staged-installer-remote-code-execution

https://www.wordfence.com/blog/2026/10/wordpress-7-1-4-security-release-rce/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 05, 2026 • 09:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com