GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

18 November 2026

Advisory 381: WordPress Core Upgrade-Window Remote Code Execution Vulnerability (CVE-2026-119977).

Release Date: 4th November 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-119977 is a time-of-check time-of-use (TOCTOU) race condition (CWE-367) in WordPress Core. During a full-package core upgrade, WordPress uses predictable, web-accessible staging paths. An unauthenticated attacker who reaches those paths during the upgrade window can run code on the server. It is rated CVSS 8.1 (High).

What are the systems affected?

The vulnerability affects self-hosted WordPress sites running:

- WordPress Core 4.7.0 through 7.1.3
- Versions 4.6 and earlier no longer receive security updates and should be treated as vulnerable

Not affected / patched version:

- WordPress 7.1.4 or later
- The fixed security release for older branches, such as 7.0.8, 6.9.11 and 6.8.12

What does this mean?

Successful exploitation may allow attackers to:

- Run code on the web server without logging in
- Install web shells and backdoors that survive later updates
- Steal database contents, user data and credentials
- Deface the site or use it to spread malware

Mitigation process

CERTVU recommends the following:

1. Update WordPress
Update every WordPress site to 7.1.4 or the fixed release for its branch. Where possible, update during low traffic, put the site in maintenance mode or restrict access to the staging directories during the update, or update with WP-CLI or a manual file replacement.

2. Check automatic updates
3. Check for compromise

Report suspected compromise to CERTVU at incident@cert.gov.vu.

Reference

1. https://wordpress.org/news/2026/10/wordpress-7-1-4/
2. https://www.cve.org/CVERecord?id=CVE-2026-119977
3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-119977