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

2 September 2026

Advisory 223: Pods WordPress Plugin Privilege Escalation Vulnerability (CVE-2026-19598).

Release Date: 15th August 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 operate WordPress websites using the Pods – Custom Content Types and Fields plugin. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-19598 is a critical privilege escalation vulnerability in the Pods WordPress plugin, located in its admin-ajax router. The router fails to properly enforce authorization on certain administrative actions, allowing an attacker who holds even a low-privileged account, such as a self-registered subscriber on a site that permits open registration, to escalate that account to administrator level.

This vulnerability is already known to be exploited in the wild, and CERTVU treats it as an active threat rather than a theoretical one. If high privileges are gained, an attacker can take full control of the affected website.

What are the systems affected?

The following version(s) are affected:

- Pods 3.3 - 3.3.9, 3.1 - 3.1.4.1, 3.2 - 3.2.8.2, 3.0 - 3.0.10.3, 2.9 - 2.9.19.3, and 2.8 - 2.8.23.3 - (Affected)

Pods 3.3.9.1 and later (and the corresponding patched point release on older branches) - (Not affected, patched)

Sites running an older Pods branch should upgrade to the latest 3.3.x release where possible, rather than only to the patched point release on their existing branch, since ongoing support is strongest on the current branch.

What does this mean?

Typical attack flow:

1. **Obtain a low-privileged account**
    - An attacker registers or otherwise obtains a low-privileged WordPress account, such as a subscriber, on a site running Pods.
2. **Escalate via the admin-ajax router**
    - The attacker sends a request to the Pods admin-ajax router that the plugin fails to properly authorize, elevating the account to administrator level.

Attack vectors:

- Any WordPress site running an affected Pods version that permits user registration, even at the lowest privilege level.
- Direct requests to the Pods admin-ajax router from an authenticated but low-privileged session.

Successful exploitation may allow attackers to:

- Escalate a low-privileged account to administrator level.
- Take full control of the affected WordPress website once administrator privileges are obtained.

Indicators of Compromise (IOCs):
This vulnerability is already known to be exploited in the wild. CERTVU draws attention to the following indicators, while noting that absence of these does not rule out compromise:

- Newly registered low-privileged (e.g. subscriber) accounts that shortly afterwards hold administrator capabilities.
- Unexpected requests to the Pods admin-ajax router in server access logs, particularly from accounts that should not hold administrative rights.
- New administrator accounts, plugin installations, or theme edits that no known staff member performed.

Mitigation process

CERTVU recommends the following:

1. Update Pods immediately

- Upgrade to Pods 3.3.9.1 or later without delay, given confirmed active exploitation.

2. Restrict or review open user registration
3. Audit WordPress user accounts
4. Audit the estate for the affected product
5. Conduct a compromise assessment

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://patchstack.com/database/wordpress/plugin/pods/vulnerability/wordpress-pods-plugin-3-3-9-unauthenticated-privilege-escalation-vulnerability
2. https://www.cve.org/CVERecord?id=CVE-2026-19598