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 224: GiveWP WordPress Donation Plugin Remote Code Execution Vulnerability (CVE-2026-82222).

Release Date: 28th 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 GiveWP donation plugin, including churches, NGOs, and non-profit organizations that collect donations online. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-82222 is a critical, maximum-severity remote code execution vulnerability in the GiveWP donation plugin, caused by unsafe handling of serialized data combined with a flawed deserialization safety mechanism. GiveWP's protective helper uses PHP's allowed_classes => false option, which was intended to reject unsafe objects but instead converts them into __PHP_Incomplete_Class placeholders that retain the original object's data.

The donation workflow allows an attacker to inject a malicious serialized object that survives this initial check and is stored in the wp_give_sessions database table. When it is later retrieved without the same restriction, PHP recreates the original malicious object, and the attacker chains this into arbitrary operating-system command execution using existing code already present in GiveWP, including its TCPDF library component.

What are the systems affected?

The following version(s) are affected:

- GiveWP 4.16.7.1 and earlier – (Affected)

GiveWP 4.16.7.2 and later – (Not affected, patched)

The fix was released 27 August 2026. Any site accepting donations through GiveWP should treat this as an urgent, internet-facing risk, since the donation form is by design accessible without authentication.

What does this mean?

Typical attack flow:

1. **Submit a crafted donation request**
    - An attacker submits a donation request containing a malicious serialized PHP object that passes GiveWP's flawed safety check and is stored in the wp_give_sessions database table.
2. **Trigger deserialization and code execution**
    - When GiveWP later retrieves and deserializes the stored session data without the same restriction, the malicious object is recreated and its gadget chain executes, resulting in arbitrary operating-system command execution with web server privileges.

Attack vectors:

- The public-facing donation form, which is accessible without authentication by design.
- No test mode, open registration, debug mode, or administrator action is required on a default GiveWP installation.

Successful exploitation may allow attackers to:

- Execute arbitrary operating-system commands with the privileges of the web server.
- Achieve full compromise of the WordPress site and, depending on server configuration, the underlying host — with no authentication required at any stage.

Mitigation process

CERTVU recommends the following:

1. Update GiveWP immediately

- Upgrade to GiveWP 4.16.7.2 or later without delay, given the maximum CVSS severity and the lack of any precondition to exploit it.

2. Review server logs for donation-form abuse
3. Restrict outbound and command execution capability
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://www.bleepingcomputer.com/news/security/givewp-wordpress-donation-plugin-flaw-lets-hackers-execute-server-commands/
2. https://www.cve.org/CVERecord?id=CVE-2026-82222