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 222: TranslatePress WordPress Plugin Unauthenticated Account Takeover Vulnerability (CVE-2026-19632).

Release Date: 26 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 multilingual WordPress websites using the TranslatePress plugin. This alert is intended to be understood by technical users and systems administrators.

CERTVU notes that TranslatePress is commonly used by sites publishing in more than one language, which may include government and public-facing sites in Vanuatu that publish in English, French and Bislama.

What is it?

CVE-2026-19632 is a critical vulnerability in the TranslatePress plugin caused by a weak password recovery mechanism. The flaw resides in the trp_get_translations_regular AJAX action, which processes both authenticated and unauthenticated requests without properly restricting access to sensitive data.

An attacker can query this AJAX endpoint directly to retrieve translation strings that contain the site administrator's raw password-reset URL and plaintext reset key. Exploitation requires the plugin's automatic string-saving feature to be enabled, which is the default setting, and the administrator's

account locale to be set to a secondary published language on the site — a combination plausible on any actively maintained multilingual site.

What are the systems affected?

The following version(s) are affected:

- TranslatePress versions up to and including 3.3.1 – (Affected)

TranslatePress 3.3.2 and later – (Not affected, patched)

Site administrators should confirm their installed TranslatePress version from the WordPress admin dashboard and upgrade regardless of whether the specific precondition combination is currently in place, since site configuration can change over time.

What does this mean?

Typical attack flow:

1. **Query the vulnerable AJAX endpoint**
    - An attacker sends an unauthenticated request directly to the trp_get_translations_regular AJAX action, which does not properly restrict which translation strings it returns.
2. **Extract the administrator's password-reset details**
    - If the site's automatic string-saving feature is enabled and the administrator account's locale is set to a secondary language, the response includes the administrator's raw password-reset URL and plaintext reset key.

Attack vectors:

- Direct, unauthenticated network requests to the AJAX endpoint — no credentials, privileges, or user interaction required.
- Any multilingual WordPress site running TranslatePress with default string-saving settings.

Successful exploitation may allow attackers to:

- Obtain the administrator's password-reset URL and reset key directly, without needing to trigger or intercept a password-reset email.
- Use the reset key to take over the administrator account and gain full control of the WordPress site.

Mitigation process

CERTVU recommends the following:

1. Update TranslatePress immediately

- Upgrade to TranslatePress 3.3.2 or later without delay.

2. Reset administrator credentials as a precaution
3. Review administrator account activity
4. Audit the estate for the affected product
5. Monitor Wordfence's and TranslatePress's security advisories for further updates

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

Reference

1. https://www.ionix.io/threat-center/cve-2026-19632/
2. https://www.cve.org/CVERecord?id=CVE-2026-19632