

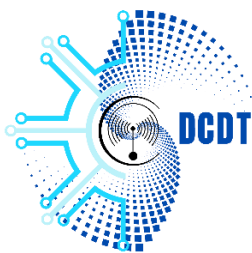
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

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

7 September 2026

Advisory 263: Frontend Admin by DynamiApps Unauthenticated Account Takeover (CVE-2026-75816).

Release Date: 5th September 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, System/Network administrators, and website teams that operate a WordPress site using the Frontend Admin by DynamiApps plugin. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-75816 is a critical, unauthenticated account-takeover vulnerability in Frontend Admin by DynamiApps, a WordPress plugin with 9,000+ active installations and a 4.5-star rating that lets site owners build front-end forms for adding and editing posts, pages, users, and Advanced Custom Fields (ACF) content without giving contributors access to the WordPress admin dashboard

What are the systems affected?

The following version(s) are affected:

- Frontend Admin by DynamiApps through 3.29.12 - (Affected)

Frontend Admin by DynamiApps 3.29.13 and later - (Not affected, patched)

What does this mean?

Typical attack flow:

1. **Submit a crafted front-end form request with a non-numeric target ID**
 - An unauthenticated attacker sends a request to one of the plugin's front-end submission endpoints, supplying a non-numeric value (such as "user_1") in place of the expected numeric post ID, which causes the plugin's `conditions_logic()` authorization check to be bypassed entirely.
2. **Overwrite the target account's email address and reset the password**
 - With the authorization check bypassed, the attacker's form submission is routed to an arbitrary WordPress user record — including an administrator account — and overwrites its registered email address to one the attacker controls. The attacker then uses WordPress's standard "lost password" flow to receive the reset link at that address and take full control of the account.

Attack vectors:

- A network-based, unauthenticated request against any internet-reachable WordPress site running an affected version of the Frontend Admin by DynamiApps plugin.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N). CERTVU is not aware of confirmed active exploitation at the time of writing, but the vulnerability requires no authentication at all and directly enables full administrator account takeover, making it an unusually high-value target for opportunistic scanning.

Successful exploitation may allow attackers to:

- Overwrite the registered email address of any WordPress user on the affected site, including an administrator, without ever holding a legitimate credential.
- Trigger WordPress's native password-reset flow to receive the reset link at an attacker-controlled address, fully taking over the targeted account — and, where the target is an administrator, gaining complete control of the WordPress site.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update the Frontend Admin by DynamiApps plugin to version 3.29.13 or later through the WordPress admin dashboard (Plugins > Installed Plugins), and confirm via the plugin's own changelog that the update addresses this account-takeover issue.

2. Treat this as urgent given the unauthenticated, no-privilege-required nature of the flaw and the direct path to full administrator account takeover
3. Audit the estate for Frontend Admin installations
4. Review administrator and other privileged accounts for unauthorized email changes
5. Review web-server access logs for suspicious activity

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

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-75816>
2. <https://wordpress.org/plugins/acf-frontend-form-element/>