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 221: Avada Theme and Fusion Builder Plugin Remote Code Execution Vulnerability (CVE-2026-18431).

Release Date: 26th 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 Avada theme together with the Fusion Builder plugin. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-18431 is a critical remote code execution vulnerability affecting sites that run both the Avada theme and the Fusion Builder plugin together. It is a broken access control flaw (CWE-862): missing authorization checks let an unauthenticated attacker write attacker-controlled files to the server.

An attacker can use this arbitrary file write to create and execute PHP files of their choosing, resulting in full remote code execution on the web server.

What are the systems affected?

The following version(s) are affected (both components must be present):

- Avada theme 7.16 and earlier - (Affected)
- Fusion Builder plugin 3.16 and earlier - (Affected)

Avada 7.16.1 and later, together with Fusion Builder 3.16.1 and later - (Not affected, patched)

Both the theme and the plugin must be updated together; updating only one leaves the site exposed. This vulnerability only applies to sites running both components — sites using Avada without Fusion Builder, or vice versa, are not affected by this specific CVE.

What does this mean?

Typical attack flow:

1. **Reach the vulnerable write path**
    - An attacker sends a request to the affected Avada/Fusion Builder functionality without any authentication, exploiting the missing authorization check to write a file to the server.
2. **Execute arbitrary PHP**
    - The attacker writes a malicious PHP file to a web-accessible location and requests it directly, achieving code execution with the privileges of the web server.

Attack vectors:

- Remote, unauthenticated network requests against any site running both Avada and Fusion Builder.
- No user interaction is required, and existing administrator-created content on the site can be enough to satisfy the precondition for exploitation.

Successful exploitation may allow attackers to:

- Write and execute arbitrary PHP code on the web server.
- Achieve full compromise of the WordPress site and, depending on server configuration, the underlying host.

Mitigation process

CERTVU recommends the following:

1. Update both Avada and Fusion Builder immediately

- Upgrade Avada to 7.16.1 or later and Fusion Builder to 3.16.1 or later. Both updates are required together.

2. Scan for planted PHP files
3. Review file integrity
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/critical-avada-wordpress-theme-flaw-enables-zero-click-rce/
2. https://www.cve.org/CVERecord?id=CVE-2026-18431