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

14 September 2026

Advisory 307: The Events Calendar WordPress Plugin Unauthenticated Remote Code Execution via Comment-Borne Object/Code Injection (CVE-2026-78006 and CVE-2026-78159).

Release Date: 12th 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 and Website administrators that operate a WordPress site using The Events Calendar plugin, particularly where public comments are enabled on event pages. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-78006 and CVE-2026-78159 are two critical, unauthenticated vulnerabilities in The Events Calendar, a WordPress event-management plugin published by StellarWP with over 600,000 active installations. Both were disclosed on 12 September 2026, affect the plugin through version 6.17.4, and were fixed together in the same release, version 6.17.4.1 - sharing the same affected scope and remediation.
CVE-2026-78006 is an insecure-deserialization flaw in the "is_safe_widget_instance" function: an attacker can bypass the plugin's object-safety check by exploiting PHP magic methods and forging a valid integrity hash.
CVE-2026-78159 is a related code-injection flaw in the "parse_array" function, where insufficient validation of a widget's "classes" map lets a plain-array payload bypass the same "is_safe_widget_instance" object check.

What are the systems affected?

The following version(s) are affected:

- The Events Calendar (WordPress plugin), all versions up to and including 6.17.4 - (Affected)

The Events Calendar, version 6.17.4.1 and later - (Not affected, patched)

Upgrade The Events Calendar plugin to version 6.17.4.1 or later without delay. Where immediate upgrading is not possible, disabling comments on event pages removes the specific attack path both vulnerabilities rely on, as an interim measure only.

What does this mean?

Typical attack flow:

1. **Submit a crafted comment on a public event page**
    - An unauthenticated attacker submits a specially crafted legacy-widget block as a public comment on any event page where comments are enabled - no account or moderation approval is required for the payload to reach the vulnerable code.
2. **Bypass object-safety validation and achieve remote code execution**
    - When the comment is processed, the plugin's "parse_array"/"is_safe_widget_instance" validation logic is bypassed - either via a forged integrity hash (CVE-2026-78006) or a plain-array payload the object check doesn't catch (CVE-2026-78159) - allowing the attacker's payload to execute arbitrary code on the server.

Attack vectors:

- A network-based, unauthenticated attack against any WordPress site running an affected version of The Events Calendar with comments enabled on event content — no account, privilege, or prior moderation approval is required.
- No user interaction beyond the attacker's own comment submission is required (CVSS UI:N), and no privileges are needed (CVSS PR:N

Successful exploitation may allow attackers to:

- Execute arbitrary code on a WordPress server hosting The Events Calendar, without any authentication, by submitting a single crafted comment.
- Fully compromise the affected WordPress site and use it as a foothold to access site data, plant further malware, or pivot into the wider hosting environment.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately

    - Upgrade The Events Calendar plugin to version 6.17.4.1 or later on every WordPress site where it is installed, as an emergency change given the unauthenticated, no-privilege attack path.

2. Disable comments on event content where patching must be delayed
3. Audit for signs of prior compromise before and after patching
4. Confirm the update reached every affected site

Report any suspected compromise of a WordPress site to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-78006
2. https://www.cve.org/CVERecord?id=CVE-2026-78159