

Alert Bulletin

Bulletin N.: 102

Publication Date: 17/09/2026

Subject: Alert 2026-102 Critical Vulnerabilities in The Events Calendar plugin for WordPress

Traffic Light Protocol (TLP): White

Affected product(s):

Product	CVE	Affected versions	Fixed version
The Events Calendar for WordPress	CVE-2026-78159	Up to 6.17.3, inclusive	6.17.3.1 or later
The Events Calendar for WordPress	CVE-2026-78006	Up to 6.17.4, inclusive	6.17.4.1 or later
The Events Calendar for WordPress	Both vulnerabilities	Versions prior to 6.17.4.1	6.17.4.1 or later

*Version **6.17.4.1**, released on September 10, 2026, is the first release that contains fixes for both vulnerabilities.

Description

Two critical remote code execution (RCE) vulnerabilities were identified in the **The Events Calendar** plugin for WordPress, developed by StellarWP. The flaws, **CVE 2026 78006** and **CVE 2026 78159**, have a **CVSS 9.8** score and allow remote unauthenticated attackers to take control of vulnerable sites under certain conditions, without requiring registration, login, or victim interaction.

The plugin has more than **600,000 active installations**. StellarWP published fixes for both vulnerability chains; it is recommended to update immediately to **The Events Calendar 6.17.4.1 or a later version** and perform a review for possible compromise, especially if the site allows comments on individual event pages.

The vulnerabilities are located in the widget rendering process of The Events Calendar, particularly when the plugin processes content from an individual event page, including comments pending moderation. The attacker does not need the comment to be approved: WordPress allows whoever published a comment to view their own pending comment through a moderation link, which can cause attacker-controlled content to reach the vulnerable plugin logic.

CVE	CVSS	Type	Main condition	Impact
-----	------	------	----------------	--------

**CVE
2026
78006**

9.8 —
Critical

PHP Object Injection

Comments enabled on event pages and “Show comments on event pages” option active

Execution of system commands and RCE with permissions of the web server user

**CVE
2026
78159**

9.8 —
Critical

Code injection via *callable invocation* / insufficient validation

Processing of controlled content within event widgets

Administrative password reset, admin access, and subsequent RCE

Solution

The definitive solution is to update **The Events Calendar** to version **6.17.4.1 or later**:

The Events Calendar

Since it is a critical RCE, easy to exploit, it is recommended after updating to follow the following verification steps:

1. Purge WordPress, PHP, CDN, and WAF caches to ensure the updated code is loaded.
2. Confirm that comments are not enabled on event pages if that functionality is not required.
3. Review administrative accounts, plugins, files, and logs to rule out prior exploitation.
4. If signs of compromise are identified, isolate the site, preserve evidence, restore from a trusted backup, and rotate credentials for WordPress, hosting, database, SFTP/SSH, APIs, and integrated services.

Additional information:

- [Wordfence — Wordfence Argus Identifies Two Critical Unauthenticated Vulnerability Chains Leading to Remote Code Execution in The Events Calendar Plugin](#)
- [Wordfence Intelligence — CVE?2026?78159](#)
- [SecurityWeek — Unauthenticated RCE Flaws Could Expose 200,000+ WordPress Sites to Takeover](#)
- [Cyber Security News — Critical WordPress Plugin Flaws Put Over 600,000 Websites at Risk of Takeover](#)