

Alert Bulletin

Bulletin N.:

Publication Date: 25/09/2026

Subject: Alert 2026-109 CSRF Vulnerability in Elementor Website Builder for WordPress

Traffic Light Protocol (TLP): Amber

Affected product(s):

Product	Affected versions	Fixed version
Elementor Website Builder for WordPress	4.3.0 and 4.3.1	4.3.2 or later
Elementor Pro	Not directly part of this advisory	Validate and apply their security updates separately

Description

A **Cross-Site Request Forgery (CSRF)** vulnerability was published in the **Elementor Website Builder** plugin for WordPress, labeled as **CVE-2026-62062 with a CVSS score of 8.8**. The flaw exclusively affects versions **4.3.0 and 4.3.1** and was fixed in version **4.3.2**, released on September 24, 2026.

CVE-2026-62062 is a **CSRF** vulnerability, classified as **CWE-352**, caused by a bypass of the WordPress REST *nonce* validation in Elementor's **Editor Events** module.

The REST *nonce* is the WordPress control designed to prevent CSRF attacks on cookie-authenticated requests. The Elementor flaw allowed any REST API endpoint to be excluded from that validation by adding the indicated text to the URL, without the requested endpoint actually belonging to `elementor/v1/events/`.

In versions 4.3.0 and 4.3.1, Elementor disables WordPress's CSRF protection for cookie-authenticated requests if it detects the literal string `elementor/v1/events/` anywhere in the request URI. Since WordPress includes the query string (*query string*) in that URI and the attacker can control the parameters of a link, an attacker can add that string to a different REST API request to cause Elementor to skip the *nonce* validation.

Additional information:

- <https://patchstack.com/articles/cross-site-request-forgery-in-elementor-plugin-affecting-2-million-sites/>
- <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/elementor/elementor-website-builder-430-431-cross-site-request-forgery-via-rest-nonce-bypass-to-privilege-escalation>

- <https://www.bleepingcomputer.com/news/security/elementor-wordpress-flaw-lets-attackers-create-admin-accounts/>