Boletín de alerta

Boletín Nro.:
Fecha de publicación: 25/09/2026
Tema: Alerta 2026-109 Vulnerabilidad CSRF en Elementor Website Builder para WordPress
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Producto	Versiones afectadas	Versión corregida
Elementor Website Builder para WordPress	4.3.0 y 4.3.1	4.3.2 o posterior
Elementor Pro	No forma parte directa de este advisory	Validar y aplicar sus actualizaciones de seguridad por separado

Descripción

Se publico una vulnerabilidad de **Cross-Site Request Forgery (CSRF)** en el plugin **Elementor Website Builder** para WordPress etiquetada como **CVE-2026-62062 con un score CVSS 8.8**. La falla afecta exclusivamente las versiones **4.3.0 y 4.3.1** y fue corregida en la versión **4.3.2**, publicada el 24 de septiembre de 2026.

CVE-2026-62062 es una vulnerabilidad de **CSRF**, clasificada como **CWE-352**, causada por un bypass de la validación del *nonce* REST de WordPress en el módulo **Editor Events** de Elementor.

El *nonce* REST es el control de WordPress diseñado para prevenir ataques CSRF en peticiones autenticadas mediante cookies. El defecto de Elementor permitía que cualquier endpoint REST API se excluyera de esa validación agregando el texto indicado a la URL, sin que el endpoint solicitado perteneciera realmente a elementor/v1/events/.

En las versiones 4.3.0 y 4.3.1, Elementor deshabilita la protección CSRF de WordPress para solicitudes autenticadas por cookies si detecta la cadena literal elementor/v1/events/ en cualquier parte de la URI de la solicitud. Dado que WordPress incluye la cadena de consulta (*query string*) en esa URI y el atacante puede controlar los parámetros de un enlace, un atacante puede añadir dicha cadena a una solicitud REST API distinta para provocar que Elementor omita la validación del *nonce*.

Información adicional:

- 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/