Alerta de seguridad cibernética	9VSA23-00922-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	17 de octubre de 2023
Última revisión	17 de octubre de 2023

NOTIFICACIÓN: La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información una vulnerabilidad crítica que afecta al plugin de WordPress conocido como Royal Elementor Addons and Templates.

Vulnerabilidades

CVE-2023-5360

Impacto

Vulnerabilidad crítica

CVE-2023-5360: Vulnerabilidad crítica que permite a atacantes autenticados subir archivos PHP incluyendo contenido malicioso, como una puerta trasera que hace posible la ejecución remota de código y lleva a un compromiso total del sitio. CVSS: 9.8.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Royal Elementor Addons and Templates anteriores a la versión 1.3.78.

Enlaces

https://www.wordfence.com/blog/2023/10/psa-critical-unauthenticated-arbitrary-file-upload-vulnerability-in-royal-elementor-addons-and-templates-being-actively-exploited/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-5360

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.17 15:11:34 -03'00'