Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00621-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2022
Última revisión	19 de abril de 2022

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 Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, advierte sobre una vulnerabilidad que afecta a Elementor, un popular plugin de WordPress (se estima que está instalado en más de cinco millones de sitios WordPress).

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2022-1329

Impacto

La vulnerabilidad es considerada **crítica** y puede llevar a la ejecución remota de código (RCE).

Productos afectados

Elementor, versiones desde la 3.6.0. y anteriores a 3.6.3.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor (versión 3.6.3 en adelante).

Enlaces

https://patchstack.com/articles/critical-vulnerability-fixed-in-elementor-plugin/
https://www.pluginvulnerabilities.com/2022/04/12/5-million-install-wordpress-plugin-elementor-contains-authenticated-remote-code-execution-rce-vulnerability/

https://www.csirt.gob.cl + (562) 24863850 @CSIRTGOB https://www.linkedin.com/company/csirt-gob