



Nro. Alerta:	EC-2022-0004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	2022/01/03	Vulnerabilidad que afecta a PowerPack para Elementor WordPress	V 1

I. DATOS GENERALES:

Clase de alerta:	Vulnerabilidad
Tipo de incidente:	Sistemas y/o software Abierto
Nivel de riesgo:	Medio

II. ALERTA

En el presente documento se dará a conocer información relacionada a CVE-2021-25027, una vulnerabilidad que afecta a PowerPack para Elementor WordPress; a continuación, se describirán parámetros técnicos de esta vulnerabilidad, el vector de ataque asociado, el impacto que produce y recomendaciones.

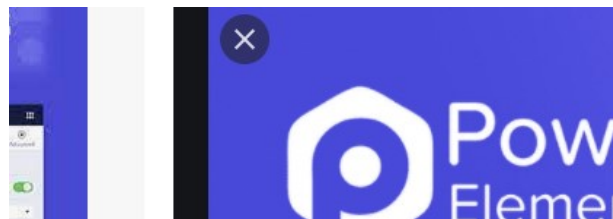


Figura 1.- Ilustraciones relacionadas a Power Pack
Fuente: Power Pack

III. INTRODUCCIÓN



CVE-2021-25027 fue publicada el 03 de enero de 2022 y la información recopilada en CVE MITRE indica que los complementos de PowerPack¹ para Elementor WordPress permanecen en el parámetro de pestaña² antes de entregar la ejecución del comando y volver al panel de administración generando un problema de secuencias de comandos entre sitios reflejados o mejor conocido como XSS (cross-site scripting vulnerabilidad que permite a un atacante insertar scripts o secuencias de código malicioso en el navegador web de un usuario.)

Es importante mencionar que, las vulnerabilidades de cross-site scripting (XSS) ocurren cuando:

¹ Uno de los complementos de Elementor con una amplia gama de widgets y plantillas premium para ayudar a crear sitios web profesionales de WordPress.

² Sistema de navegación para ordenar el contenido en tu sitio de WordPress



Nro. Alerta:	EC-2022-0004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	
TLP:	 TLP:BLANCO		
Fecha:	2022/01/03	Vulnerabilidad que afecta a PowerPack para Elementor WordPress	V 1

- Los datos que no son de confianza ingresan a una aplicación web, generalmente desde una solicitud web.
- La aplicación web genera dinámicamente una página web que contiene estos datos que no son de confianza. **[CVE 2021-25027]**
- Durante la generación de la página, la aplicación no evita que los datos contengan contenido ejecutable por un navegador web, como JavaScript, etiquetas HTML, atributos HTML, eventos de mouse, Flash, ActiveX, etc.
- Una víctima visita la página web generada a través de un navegador web, que contiene un script malicioso que se inyectó con datos que no son de confianza.
- Dado que el script proviene de una página web enviada por el servidor web, el navegador web de la víctima ejecuta el script malicioso en el contexto del dominio del servidor web.
- Esto viola efectivamente la intención de la política del mismo origen del navegador web, que establece que los scripts en un dominio no deberían poder acceder a recursos o ejecutar código en un dominio diferente.

Esta vulnerabilidad afecta a versiones anteriores a 2.6.2 y revisando la línea de tiempo se tiene que una vulnerabilidad asociada fue detectada el 2021-12-06.

IV. VECTOR DE ATAQUE: Red/RCE



El ataque puede ser iniciado desde la red.

V. IMPACTO:

Una vez que se inyecta el script malicioso, el atacante puede realizar una variedad de actividades maliciosas, el atacante podría transferir información privada, como cookies que pueden incluir información de sesión, desde la máquina de la víctima al atacante; así mismo, el ataque más común realizado con secuencias de comandos entre sitios implica la divulgación de información almacenada en las cookies de los usuarios.

En este sentido, la Confidencialidad es notablemente afectada.



Nro. Alerta:	EC-2022-0004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	
TLP:	 TLP:BLANCO		
Fecha:	2022/01/03	Vulnerabilidad que afecta a PowerPack para Elementor WordPress	V 1

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo actualizar “PowerPack Addons for Elementor” a la versión 2.6.2.

VII. REFERENCIAS:

CVE. (03 de 01 de 2022). Obtenido de CVE: <https://www.cve.org/CVERecord?id=CVE-2021-25027>

DATABASE, N. V. (03 de 01 de 2022). *NATIONAL VULNERABILITY DATABASE*. Obtenido de <https://nvd.nist.gov/vuln/detail/CVE-2021-25027>

Masterplugins. (s.f.). *Masterplugins*. Obtenido de Masterplugins: <https://masterplugins.com/producto/elementos-de-powerpack-para-elementor/>

MITRE, C. (03 de 01 de 2022). *CVE MITRE*. Obtenido de CVE MITRE: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25027>

MITRE, C. (s.f.). *CVE MITRE*. Obtenido de CVE MITRE: <http://cwe.mitre.org/data/definitions/79.html>

Vuldb. (03 de 01 de 2022). *Vuldb*. Obtenido de <https://vuldb.com/es/?id.189600>

