	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 081	Fecha: 04-04-2023
		Página 9 de 27

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Explotación activa de vulnerabilidad de WordPress Elementor Pro.		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

ANTECEDENTES:

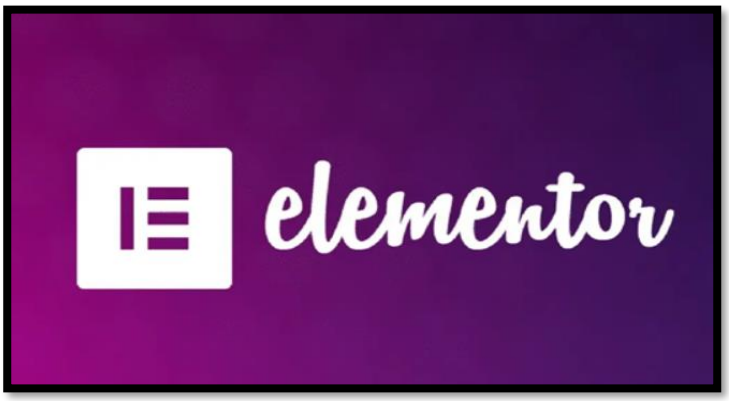
El 01 de abril del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se descubrió que, los ciberdelincuentes están explotando activamente una vulnerabilidad de seguridad parcheada recientemente en el complemento del creador de sitios web Elementor Pro para WordPress.

DETALLES:

La vulnerabilidad ha sido calificada como crítica con una calificación de gravedad de 8,8 de un máximo de 10 puntos. Esta falla fue descrita como un caso de control de acceso roto que afecta a las versiones 3.11.6 y anteriores.

La explotación exitosa de la falla de alta gravedad permite que un atacante autenticado complete una toma de control de un sitio de WordPress que tiene habilitado WooCommerce. La vulnerabilidad de control de acceso roto se deriva del uso de Elementor Pro del componente "elementor-pro/modules/woocommerce/module.php".

Esto hace posible que un usuario malicioso active la página de registro (si está deshabilitada) y establezca el rol de usuario predeterminado en administrador para que pueda crear una cuenta que tenga privilegios de administrador. Después de esto, es probable que redirijan el sitio a otro dominio malicioso o carguen un complemento malicioso o una puerta trasera para explotar aún más el sitio.



La falla está siendo abusada actualmente desde varias direcciones IP con la intención de cargar archivos PHP y ZIP arbitrarios.

RECOMENDACIONES:

- Se recomienda que actualice Elementor Pro a la versión 3.11.7 o posterior (la última disponible es la 3.12.0) lo antes posible, para mitigar posibles amenazas.
- Si emplea WordPress en su página web se recomienda ir a la sección plugins, revisar si existe una versión nueva de los plugins para actualizar.

Fuentes de información	▪ hxxps://thehackernews.com/2023/04/hackers-exploiting-wordpress-elementor.html