BOLETÍN DE ALERTA

Boletín Nro.: 2023-13
Fecha de publicación: 03/04/2023
Tema: Vulnerabilidad de acceso no autorizado en *plugin* Elementor Pro de WordPress

Software afectado:

- *Plugin* Elementor Pro, versión 3.11.6 y anteriores.

  Obs: sólo es afectada la versión Pro de Elementor, no así la versión gratuita.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad explotada activamente que afecta al *plugin* Elementor Pro de WordPress, que permitiría a un atacante autenticado crear una cuenta de administrador, acceder a registros confidenciales y obtener acceso no autorizado del sistema afectado.

La vulnerabilidad identificada sin CVE asignada aún, de severidad “Alta” y con puntuación asignada de 8.8. Esta vulnerabilidad se debe a una falla de validación de entradas del usuario al implementar la acción *AJAX* "*pro_woocommerce_update_page_option*" en el *plugin* Elementor Pro de WordPress. Esto permitiría a un atacante autenticado a través de un control de acceso incorrecto dentro del *plugin* WooCommerce del módulo "*elementor-pro /modules/woocommerce/module.php*" (cuando el mismo se encuentre habilitado), crear una cuenta de administrador, habilitar y establecer el rol predeterminado de administrador, realizar modificaciones a la base de datos y obtener el control total del sitio afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante autenticado obtener información confidencial y el acceso no autorizado al sistema afectado.

Prevención:

Agregar las siguientes direcciones IP públicas a listas negras de los dispositivos de comunicación de la organización:

- 193.169.194.63
- 193.169.195.64
- 194.135.30.6

Detección:

Identificar en los registros de acceso *HTTP* dominios maliciosos ("*away[.]trackersline[.]com*").

Identificar puertas traseras en el sitio afectado llamadas:

- *wp-resortpark.zip*

- *wp-rate.php*
- *lll.zip*

Identificar registros de acceso en los dispositivos de comunicación las direcciones *IP* públicas mencionadas en la sección de prevención.

Solución:

Recomendamos instalar la actualización correspondiente provista por el fabricante, mediante en el siguiente enlace:

- https://elementor.com/pro/changelog/

Información adicional:

- https://www.bleepingcomputer.com/news/security/hackers-exploit-bug-in-elementor-pro-wordpress-plugin-with-11m-installs/
- https://blog.nintechnet.com/high-severity-vulnerability-fixed-in-wordpress-elementor-pro-plugin/
- https://patchstack.com/articles/critical-elementor-pro-vulnerability-exploited/
- https://patchstack.com/database/vulnerability/elementor-pro/wordpress-elementor-pro-3-11-6-authenticated-arbitrary-options-change-vulnerability
- https://elementor.com/pro/changelog/