Se descubrió que Elementor, un complemento de creación de sitios web de WordPress, con más de cinco millones de instalaciones activas, es vulnerable a una falla de ejecución de código remoto autenticado que podría abusarse para hacerse cargo de los sitios web afectados.

La vulnerabilidad del plugin, que fue revelada la semana pasada, se introdujo en la versión 3.6.0 que se lanzó el 22 de marzo de 2022. Aproximadamente el 37% de los usuarios del complemento se encuentran en la versión 3.6.x.

> *«Esto significa que el sitio web puede ejecutar código malicioso proporcionado por el atacante. En este caso, es posible que alguien que no haya iniciado sesión en WordPress pueda explotar la vulnerabilidad, pero cualquiera que haya iniciado sesión en WordPress y tenga acceso al panel de administración de WordPRess puede explotarla fácilmente»,* dijeron los investigadores.

El problema se relaciona con un caso de carga arbitraria de archivos en los sitios web afectados, lo que podría conducir a la ejecución del código.

La vulnerabilidad fue corregida en la última versión de Elementor, y Patchstack dijo que *«esta vulnerabilidad podría permitir que cualquier usuario autenticado, independientemente de su autorización, cambie el título del sitio, el logotipo del sitio, cambie el tema de Elementor y lo peor de todo, cargue archivos arbitrarios en el sitio».*

La divulgación se produce más de dos meses después de que se descubrió que Essential Addons para Elementor contenía una vulnerabilidad crítica que podría resultar en la ejecución de código arbitrario en sitios web comprometidos.