Se ha descubierto que un plugin de WordPress con más de un millón de instalaciones, contiene una vulnerabilidad crítica que podría resultar en la ejecución de código arbitrario en sitios web comprometidos.

El complemento es Essential Addons for Elementor, que brinda a los propietarios de sitios web en WordPress una biblioteca de más de 80 elementos y extensiones para ayudar a diseñar y personalizar páginas y publicaciones.

> *«Esta vulnerabilidad permite que cualquier usuario, independientemente de su estado de autenticación o autorización, realice un ataque de inclusión de archivos locales. Este ataque se puede usar para incluir archivos locales en el sistema de archivos del sitio web, como /etc/password. Esto también puede utilizarse para realizar RCE al incluir un archivo con código PHP malicioso que normalmente no se puede ejecutar»,* dijo Patchstack en un informe.

La vulnerabilidad solo existe si se utilizan widgets como la galería dinámica y la galería de productos, que utilizan la función vulnerable, lo que resulta en la inclusión de archivos locales, una técnica de ataque en la que se engaña a una aplicación web para que exponga o ejecute archivos arbitrarios en el servidor web.

La vulnerabilidad afecta a todas las versiones del complemento a partir de la 5.0.4 y anteriores, y se la atribuye el descubrimiento de la vulnerabilidad al investigador Wai Yan Myo Thet. Luego de la divulgación responsable, la brecha de seguridad fue corregida en la versión 5.0.5 lanzada el 28 de enero *«después de varios parches insuficientes».*

El desarrollo se produce unas semanas después de que se informó que actores no identificados manipularon docenas de temas y plugins de WordPress alojados en el sitio web de un desarrollador para inyectar una backdoor con el objetivo de infectar más sitios.