Investigadores de Wordfence emitieron una alerta sobre un aumento *«repentino»* en los ataques cibernéticos que intentan explotar una vulnerabilidad sin parchear en un complemento de WordPress llamado Kaswara Modern WPBakery Page Builder Addons.

Rastreada como CVE-2021-24284, la vulnerabilidad tiene una calificación de 10.0 en el sistema de calificación de vulnerabilidades CVSS, y se relaciona con la carga de un archivo arbitrario no autenticado que podría abusarse para obtener la ejecución de código, lo que permite a los atacantes tomar el control de los sitios de WordPress afectados.

Aunque el error fue revelado originalmente en abril de 2021 por la compañía de seguridad de WordPress, sigue sin resolverse hasta ahora. Para empeorar todo, el complemento se ha cerrado y ya no se mantiene activo.

Wordfence, que protege más de 1000 sitios web que tienen instalado el plugin, dijo que bloqueó un promedio de 443,868 intentos de ataque por día desde principios del mes.

Los ataques han emanado de 10,215 direcciones IP, con la mayoría de los intentos de explotación reducidos a 10 direcciones IP. Estos implican la carga de un archivo ZIP que contiene un archivo PHP malicioso que permite al atacante cargar archivos falsos en el sitio web infectado.

El objetivo de la campaña parece ser la inserción de código en archivos JavaScript legítimos y redirigir a los visitantes del sitio a sitios web maliciosos. Cabe mencionar que los ataques han sido rastreados por Avast y Sucuri bajo los nombres de Parrot TDS y NDSW, respectivamente.

Se cree que entre 4000 y 8000 sitios web tienen instalado el complemento, por lo que es imperativo que los usuarios lo eliminen de sus sitios de WordPress para frustrar posibles ataques y encontrar una alternativa adecuada.