Plugin De Análisis Para WordPress Deja Vulnerable A Una Gran Cantidad De Sitios Web

Una vulnerabilidad peligrosa ha sido descubierta en uno de los **plugins más populares**, WordPress. Esta vulnerabilidad pone más de un millón de sitios web en riesgo de ser completamente secuestrado por los atacantes.

La vulnerabilidad reside realmente en la mayoría de las versiones de un plugin de WordPress llamado **Wettable Powder Slimstat (WP-Slimstat)**. Si bien existe más de 70 millones de sitios web en Internet que están usando WordPress, más de 1,3 millones de ellos utilizan el Plugin «WP-SLIMStat ‘, por lo que es uno de los **plugins más populares de WordPress** para un potente análisis web en tiempo real.

Todas las **versiones de WP-SLIMStat** anteriores a la última versión de 3.9.6 contienen una clave «secreta» fácil de adivinar, la cual se utiliza para firmar los datos enviados desde los equipos de los usuarios que visitan el sitio, explicaron en un blog publicado el martes por la empresa de seguridad web, Sucuri.

Una vez que la clave es obtenida, un atacante podría ejecutar un ataque de inyección SQL en el sitio web de destino con el fin de apoderarse de información altamente sensible de la base de datos de la víctima, incluyendo contraseñas encriptadas y claves de cifrado utilizadas para administrar remotamente los sitios web.

> *«Si su sitio web utiliza una versión vulnerable del plugin, estás en riesgo», Marc-Alexandre Montpas, investigador senior de la vulnerabilidades en Sucuri, escribió.*

> *«Una explotación exitosa de este fallo podría dar lugar a ataques de inyección SQL a ciegas, lo que significa que un atacante podría tomar la información sensible de su base de datos, incluyendo nombre de usuario, (hash) contraseñas y, en ciertas configuraciones de WordPress, claves secretas (que podría resultar en un sitio totales tomar el control). «*

Esto deja a un atacante con cerca de 30 millones de sitios para poner a prueba, que podrían completarse en unos 10 minutos con la mayoría de las CPU modernas. Una vez que la clave secreta ha sido detectada, el atacante puede utilizar la clave para obtener los datos sensibles de la base de datos.

Si eres uno de los usuarios que usan **WP-Slimstat en WordPress**, no dudes en actualizar a la nueva versión, con esto podrás evitar que tu sitio web sea tomado bajo el control de atacantes informáticos.