Dos vulnerabilidades críticas de seguridad afectan al plugin de protección contra spam, Anti-Spam y Firewall de WordPress, lo que podría permitir que un atacante sin autenticación instale y active plugins maliciosos en sitios vulnerables, llegando incluso a ejecutar código de forma remota.

Estas fallas, identificadas como CVE-2024-10542 y CVE-2024-10781, obtuvieron una calificación CVSS de 9.8 sobre 10. Las correcciones para ambas se implementaron en las versiones 6.44 y 6.45, lanzadas este mes.

El plugin de CleanTalk, utilizado en más de 200,000 sitios de WordPress, se describe como una solución *«universal contra el spam»,* diseñada para bloquear comentarios, registros y encuestas no deseados, entre otras amenazas.

De acuerdo con Wordfence, ambas vulnerabilidades están relacionadas con problemas que permiten omitir medidas de autorización, posibilitando que un atacante instale y active plugins arbitrarios. Si uno de estos plugins presenta fallos de seguridad, podría facilitar la ejecución remota de código malicioso.

El investigador de seguridad István Márton explicó que la vulnerabilidad CVE-2024-10781 surge de la falta de validación del valor ‘api_key’ en la función ‘perform’, lo que afecta a todas las versiones del plugin hasta la 6.44 inclusive.

Por su parte, la CVE-2024-10542 explota una omisión de autorización mediante una suplantación del DNS inverso en la función checkWithoutToken().

Explotar con éxito estas vulnerabilidades permitiría al atacante no solo instalar y activar plugins, sino también desactivarlos o incluso desinstalarlos.

Los administradores que usen este plugin deben actualizarlo inmediatamente a las versiones parcheadas para proteger sus sitios de posibles ataques.

Además, Sucuri ha advertido sobre campañas activas que comprometen sitios de WordPress

para inyectar código malicioso. Este código puede redirigir a los visitantes hacia páginas fraudulentas, robar credenciales, instalar malware que capture contraseñas de administrador, dirigir a estafas como las de VexTrio Viper y ejecutar código PHP arbitrario en los servidores afectados.