Una nueva falla de seguridad ha sido identificada en el plugin OttoKit (anteriormente conocido como SureTriggers) para WordPress, y ya está siendo aprovechada por atacantes en entornos reales.

Esta vulnerabilidad, identificada como CVE-2025-27007 con una puntuación CVSS de 9.8, permite la escalada de privilegios y afecta a todas las versiones del complemento hasta la 1.0.82 inclusive.

Según Wordfence, *«el problema se origina porque la función `create_wp_connection()` no realiza una verificación adecuada de capacidades ni valida correctamente las credenciales del usuario»*. Esto permite que actores no autenticados puedan establecer una conexión, lo cual puede llevar a obtener privilegios más altos de forma no autorizada.

No obstante, el fallo solo puede ser explotado en dos situaciones específicas:

1. Cuando el sitio nunca ha utilizado contraseñas de aplicación, y OttoKit tampoco ha sido vinculado mediante una de estas contraseñas.
2. Si el atacante ya tiene acceso autenticado al sitio y puede generar una contraseña de aplicación válida.

Wordfence también informó que los atacantes están intentando explotar esta vulnerabilidad para establecer una conexión inicial con el sitio y, posteriormente, crear cuentas de administrador utilizando el punto de acceso de automatización/acción del plugin.

Además, se ha detectado que los mismos ataques buscan aprovechar otra falla distinta del complemento, identificada como CVE-2025-3102 (con puntuación CVSS de 8.1), la cual también ha sido objeto de explotación activa desde el mes pasado.

Esto sugiere que los actores maliciosos están realizando escaneos masivos de instalaciones WordPress para detectar si son vulnerables a una de estas dos fallas. Las siguientes direcciones IP han sido identificadas como origen de estos intentos:

- 2a0b:4141:820:1f4::2
- 41.216.188.205
- 144.91.119.115
- 194.87.29.57
- 196.251.69.118
- 107.189.29.12
- 205.185.123.102
- 198.98.51.24
- 198.98.52.226
- 199.195.248.147

Dado que el complemento cuenta con más de 100,000 instalaciones activas, es fundamental que los usuarios actualicen de inmediato a la versión 1.0.83, que soluciona estos problemas.

Wordfence advirtió que los ataques podrían haber comenzado tan temprano como el 2 de mayo de 2025, intensificándose a gran escala desde el 4 de mayo de 2025.