Una vulnerabilidad crítica de seguridad en el tema Bricks para WordPress está siendo explotada activamente por actores maliciosos para ejecutar código PHP arbitrario en instalaciones vulnerables.

Esta vulnerabilidad, identificada como CVE-2024-25600 (puntuación CVSS: 9.8), permite a atacantes no autenticados lograr la ejecución remota de código. Afecta a todas las versiones de Bricks hasta la 1.9.6, incluyendo esta última.

Los desarrolladores del tema han abordado esta cuestión en la versión 1.9.6.1, lanzada el 13 de febrero de 2024, apenas unos días después de que la empresa de seguridad Snicco informara sobre la vulnerabilidad el 10 de febrero.

Aunque aún no se ha publicado un exploit de prueba de concepto (PoC), tanto Snicco como Patchstack han compartido detalles técnicos, señalando que el código vulnerable se encuentra en la función *prepare_query_vars_from_settings().*

En términos concretos, la vulnerabilidad se relaciona con el uso de tokens de seguridad llamados «*nonces*» para verificar permisos, que luego pueden utilizarse para enviar comandos arbitrarios para su ejecución, permitiendo efectivamente que un actor malicioso tome el control de un sitio objetivo.

El valor de nonce está disponible públicamente en el frontend de un sitio de WordPress, según Patchstack, y añadieron que no se aplican verificaciones adecuadas de roles.

> *«Los nonces nunca deben ser la única medida de autenticación, autorización o control de acceso. Protege tus funciones utilizando current_user_can() y siempre asume que los nonces pueden ser comprometidos»,* advierte WordPress en su documentación.

La compañía de seguridad de WordPress, Wordfence, informó haber detectado más de tres docenas de intentos de ataque que explotan esta vulnerabilidad hasta el 19 de febrero de

2024. Se dice que los intentos de explotación comenzaron el 14 de febrero, un día después de la divulgación pública.

La mayoría de los ataques provienen de las siguientes direcciones IP:

- 200.251.23[.]57
- 92.118.170[.]216
- 103.187.5[.]128
- 149.202.55[.]79
- 5.252.118[.]211
- 91.108.240[.]52

Se estima que Bricks cuenta con alrededor de 25,000 instalaciones activas en la actualidad. Se recomienda a los usuarios del plugin que apliquen los últimos parches para mitigar posibles amenazas.