Se realizado una actualización automática de un plugin ampliamente utilizado en sitios web de WordPress, llamado Ninja Forms, con el fin de corregir una vulnerabilidad de seguridad crítica que se sospecha, ha estado siendo explotada activamente en la naturaleza.

La vulnerabilidad, que se relaciona con un caso de inyección de código, tiene una calificación de 9.8 sobre 10 en gravedad, y afecta a varias versiones a partir de la 3.0. Se ha corregido en 3.0.34.2, 3.1.10, 3.2.28, 3.3.21.4, 3.4.34.2, 3.5.8.4 y 3.6.11.

Ninja Forms es un generador de formularios de contacto personalizable que cuenta con más de 1 millón de instalaciones.

Según Wordfence, el error *«hizo posible que los atacantes no autenticados llamaran a un número limitado de métodos en varias clases de Ninja Forms, incluido un método que no serializaba el contenido proporcionado por el usuario, lo que resultaba en la inyección de objetos».*

> *«Esto podría permitir a los atacantes ejecutar código arbitrario o eliminar archivos arbitrarios en sitios donde estaba presente una cadena separada [de programación orientada a la propiedad]»,* dijo Chloe Chamberland, de Wordfence.

La explotación exitosa de la vulnerabilidad podría permitir que un atacante logre la ejecución remota de código y se apodere completamente de un sitio web vulnerable de WordPress.

Se recomienda a los usuarios de Ninja Forms que se aseguren de que sus sitios de WordPress estén actualizados para ejecutar la última versión parcheada para evitar posibles intentos de explotación.