Se ha divulgado una vulnerabilidad de seguridad crítica en el plugin multilingüe WPML de WordPress, que podría permitir a usuarios autenticados ejecutar código arbitrario de manera remota bajo ciertas condiciones.

La vulnerabilidad, identificada como CVE-2024-6386 (con una puntuación CVSS de 9.9), afecta a todas las versiones del plugin anteriores a la 4.6.13, la cual se lanzó el 20 de agosto de 2024.

Este problema surge debido a la falta de validación y limpieza de las entradas, lo que permite a atacantes autenticados, con permisos de nivel de Contribuidor o superior, ejecutar código en el servidor.

WPML es un plugin ampliamente utilizado para construir sitios web multilingües en WordPress, con más de un millón de instalaciones activas.

El investigador de seguridad stealthcopter, quien descubrió y reportó la vulnerabilidad CVE-2024-6386, señaló que el fallo se encuentra en la forma en que el plugin maneja los shortcodes, que se usan para insertar contenido en las publicaciones, como audio, imágenes y videos.

«El plugin utiliza plantillas Twig para renderizar contenido en los shortcodes, pero no realiza un saneamiento adecuado de las entradas, lo que provoca una inyección de plantillas en el servidor (SSTI)», explicó el investigador.

La SSTI ocurre cuando un atacante puede utilizar la sintaxis nativa de una plantilla para inyectar una carga maliciosa en la plantilla web, que luego se ejecuta en el servidor. Esto podría permitir al atacante ejecutar comandos arbitrarios, otorgándole el control total del sitio.

> *«Esta versión de WPML corrige una vulnerabilidad de seguridad que podría permitir a usuarios con ciertos permisos realizar acciones no autorizadas. Es poco probable*

> *que este problema se presente en situaciones reales, ya que requiere que los usuarios tengan permisos de edición en WordPress y que el sitio tenga una configuración muy específica»,* explicaron los desarrolladores del plugin, OnTheGoSystems.

Se recomienda a los usuarios del plugin aplicar las actualizaciones más recientes para reducir el riesgo de posibles amenazas.