La red social descentralizada Mastodon ha dado a conocer una vulnerabilidad crítica de seguridad que permite a actores maliciosos suplantar y tomar el control de cualquier cuenta.

> *«Debido a la insuficiente validación de origen en todo Mastodon, los atacantes pueden hacerse pasar y apoderarse de cualquier cuenta remota»,* indicaron los responsables en un breve aviso.

La vulnerabilidad, identificada como CVE-2024-23832, tiene una calificación de gravedad de 9.4 sobre un máximo de 10. Se atribuye al investigador de seguridad arcanicanis por descubrirla y reportarla.

Se describe como un *«error de validación de origen»* (CWE-346), que comúnmente permite a un atacante *«acceder a cualquier funcionalidad inadvertidamente accesible desde la fuente».*

Cualquier versión de Mastodon anterior a la 3.5.17 es vulnerable, al igual que las versiones 4.0.x anteriores a la 4.0.13, las versiones 4.1.x anteriores a la 4.1.13 y las versiones 4.2.x anteriores a la 4.2.5.

Mastodon ha anunciado que retendrá detalles técnicos adicionales sobre la falla hasta el 15 de febrero de 2024, para brindar a los administradores suficiente tiempo para actualizar las instancias del servidor y prevenir la probabilidad de explotación.

> *«Proporcionar cualquier cantidad de detalles facilitaría la creación de un exploit»,* afirmaron.

La naturaleza federada de la plataforma significa que opera en servidores separados (también conocidos como instancias), alojados y operados de forma independiente por administradores respectivos que establecen sus propias reglas y regulaciones aplicables localmente.

Esto implica que cada instancia no solo tiene un código de conducta, términos de servicio, política de privacidad y pautas de moderación de contenido únicos, sino que también requiere que cada administrador aplique actualizaciones de seguridad de manera oportuna para proteger las instancias contra posibles riesgos.

La divulgación se produce aproximadamente siete meses después de que Mastodon abordara otras dos vulnerabilidades críticas (CVE-2023-36460 y 2023-36459) que podrían haber sido aprovechadas por adversarios para provocar una denegación de servicio (DoS) o lograr la ejecución remota de código.