Mastodon Social Network lanzó actualizaciones de seguridad para corregir vulnerabilidades críticas que permiten la toma de control del servidor

Mastodon, una popular red social descentralizada, ha lanzado una actualización de seguridad para resolver vulnerabilidades críticas que podrían exponer a millones de usuarios a posibles ataques.

Mastodon es conocido por su modelo federado, que consiste en miles de servidores separados llamados *«instancias»,* y cuenta con más de 14 millones de usuarios en más de 20,000 instancias.

La vulnerabilidad más crítica, identificada como CVE-2023-36460, permite a los hackers aprovechar una falla en la función de archivos adjuntos de medios, creando y sobrescribiendo archivos en cualquier ubicación que el software pueda acceder en una instancia.

Esta vulnerabilidad de software podría ser utilizada para ataques de denegación de servicio (DoS) y ejecución remota de código arbitrario, representando una amenaza significativa para los usuarios y el ecosistema de Internet en general.

Si un atacante obtiene el control de múltiples instancias, podría causar daño al instruir a los usuarios a descargar aplicaciones maliciosas o incluso derribar toda la infraestructura de Mastodon. Afortunadamente, no hay evidencia de que esta vulnerabilidad haya sido explotada hasta ahora.

La falla crítica fue descubierta como parte de una exhaustiva iniciativa de pruebas de penetración financiada por la Fundación Mozilla y llevada a cabo por Cure53.

La reciente actualización de parche abordó cinco vulnerabilidades, incluyendo otro problema crítico conocido como CVE-2023-36459. Esta vulnerabilidad podría permitir a los atacantes insertar HTML arbitrario en las tarjetas de vista previa de oEmbed, eludiendo el proceso de saneamiento de HTML de Mastodon.

Como resultado, se introdujo una vía para cargas de Cross-Site Scripting (XSS) que podrían ejecutar código malicioso cuando los usuarios hicieran clic en las tarjetas de vista previa

asociadas con enlaces maliciosos.

Las otras tres vulnerabilidades fueron clasificadas como de gravedad alta y media. Incluían *«Inyección LDAP ciega en el inicio de sesión»,* lo cual permitía a los atacantes extraer atributos arbitrarios de la base de datos LDAP, *«Denegación de servicio a través de respuestas HTTP lentas»* y un problema de formato con *«Enlaces de perfil verificados»*. Cada una de estas debilidades presentaba diferentes niveles de riesgo para los usuarios de Mastodon.

Para protegerse, los usuarios de Mastodon solo necesitan asegurarse de que la instancia a la que están suscritos haya instalado las actualizaciones necesarias de manera oportuna.