Investigadores en ciberseguridad han descubierto seis vulnerabilidades en el marco de inteligencia artificial (IA) de Ollama que podrían ser aprovechadas por un atacante para realizar diversas actividades maliciosas, como ataques de denegación de servicio (DoS), manipulación de modelos y robo de modelos.

> *«En conjunto, estas vulnerabilidades permiten que un atacante realice un amplio abanico de acciones maliciosas con una sola solicitud HTTP, tales como ataques DoS, manipulación de modelos y robo de modelos, entre otras»,* explicó Avi Lumelsky, investigador de Oligo Security, en un informe publicado la semana pasada.

Ollama es una aplicación de código abierto que permite a los usuarios desplegar y operar modelos de lenguaje de gran tamaño (LLMs) localmente en dispositivos con Windows, Linux y macOS. Hasta la fecha, su repositorio en GitHub ha sido bifurcado 7,600 veces.

A continuación se ofrece un resumen de las seis vulnerabilidades:

- CVE-2024-39719 (Puntuación CVSS: 7.5): Una vulnerabilidad que permite a un atacante utilizar el endpoint `/api/create` para verificar si un archivo existe en el servidor (Solucionado en la versión 0.1.47).
- CVE-2024-39720 (Puntuación CVSS: 8.2): Una vulnerabilidad de lectura fuera de límites que podría causar un fallo en la aplicación mediante el endpoint `/api/create`, generando una condición de DoS (Solucionado en la versión 0.1.46).
- CVE-2024-39721 (Puntuación CVSS: 7.5): Una vulnerabilidad que genera un agotamiento de recursos y, finalmente, un DoS cuando se invoca repetidamente el endpoint `/api/create` con el archivo «/dev/random» como entrada (Solucionado en la versión 0.1.34).
- CVE-2024-39722 (Puntuación CVSS: 7.5): Una vulnerabilidad de recorrido de rutas en el endpoint `api/push`, que permite acceder a los archivos presentes en el servidor y a toda la estructura de directorios donde se despliega Ollama (Solucionado en la versión 0.1.46).

- Una vulnerabilidad que puede llevar a la manipulación de modelos a través del endpoint `/api/pull` desde una fuente no confiable (Sin identificador CVE, Sin parche).
- Una vulnerabilidad que podría permitir el robo de modelos mediante el endpoint `/api/push` hacia un destino no confiable (Sin identificador CVE, Sin parche).

Para las dos vulnerabilidades no solucionadas, los mantenedores de Ollama han recomendado que los usuarios controlen los endpoints expuestos a internet mediante un proxy o firewall de aplicaciones web.

> *«Esto implica que, de manera predeterminada, no todos los endpoints deberían estar expuestos. Es una suposición peligrosa, ya que no todos son conscientes de la necesidad de filtrar el enrutamiento HTTP hacia Ollama. Actualmente, estos endpoints están disponibles en el puerto predeterminado de Ollama en cada despliegue, sin separación ni documentación que lo respalde»,* señaló Lumelsky.

Oligo informó haber encontrado 9,831 instancias únicas con acceso a internet que ejecutan Ollama, la mayoría ubicadas en China, EE. UU., Alemania, Corea del Sur, Taiwán, Francia, Reino Unido, India, Singapur y Hong Kong. Se considera que uno de cada cuatro servidores con acceso a internet es vulnerable a los fallos identificados.

Este hallazgo llega más de cuatro meses después de que la firma de seguridad en la nube Wiz divulgara una grave vulnerabilidad en Ollama (CVE-2024-37032) que podría haber permitido la ejecución remota de código.

> *«Exponer Ollama a internet sin medidas de autorización es similar a exponer el socket de Docker en la red pública, ya que permite cargar archivos y tiene capacidades de extracción y envío de modelos (que los atacantes pueden abusar)»,* explicó Lumelsky.