关于 Ollama 存在未授权访问漏洞的安全公告

2025-03-01 17:25:09

安全公告编号:CNTA-2025-0003

近日，国家信息安全漏洞共享平台（CNVD）收录了 Ollama 未授权访问漏洞（CNVD-2025-04094）。未经授权的攻击者可以远程访问 Ollama 服务接口执行敏感资产获取、虚假信息投喂、拒绝服务等恶意操作。CNVD 建议受影响的单位和用户立即采取措施防范漏洞攻击风险。

一、漏洞情况分析

Ollama 是一个本地私有化部署大语言模型（LLM，如 DeepSeek 等）的运行环境和平台，简化了大语言模型在本地的部署、运行和管理过程，具有简化部署、轻量级可扩展、API 支持、跨平台等特点，在 AI 领域得到了较为广泛的应用。

Ollama 存在未授权访问漏洞。由于 Ollama 默认未设置身份验证和访问控制功能，未经授权的攻击者可在远程条件下调用 Ollama 服务接口，执行包括但不限于敏感模型资产窃取、虚假信息投喂、模型计算资源滥用和拒绝服务、系统配置篡改和扩大利用等恶意操作。未设置身份验证和访问控制功能且暴露在公共互联网上的 Ollama 易受此漏洞攻击影响。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

漏洞影响的产品和版本：

Ollama 所有版本（未设置访问认证的情况下）

三、漏洞处置建议

请使用 Ollama 部署大模型的单位和用户立即采取以下措施进行漏洞修复：

1、若 Ollama 只提供本地服务，设置环境变量 Environment="OLLAMA_HOST=127.0.0.1"，仅允许本地访问

2、若 Ollama 需提供公网服务，选择以下方法添加认证机制：

1）修改 config.yaml、settings.json 配置文件，限定可访问 Ollama 服务的 IP 地址；

2）通过防火墙等设备配置 IP 白名单，阻止非授权 IP 的访问请求；

3）通过反向代理进行身份验证和授权（如使用 OAuth2.0 协议），防止未经授权用户访问。