Sécurité des serveurs LLM auto-hébergés : le cas Ollama

L'outil open source Ollama permet de déployer facilement des modèles de langage (LLM) en local. Mais cette simplicité cache un risque : plus de 1 100 serveurs sont exposés sur Internet sans authentification, selon Cisco Talos. Parmi eux, 214 hébergent des modèles actifs comme Mistral ou LLaMA, accessibles librement. Cette situation soulève des enjeux critiques de cybersécurité. Comment une telle exposition est-elle possible et quelles en sont les conséquences L'analyse de Cisco Talos s'est appuyée sur le moteur de recherche Shodan pour identifier les serveurs en écoute sur le port par défaut d'Ollama (11434). Des requêtes simples ont ensuite été envoyées pour tester l'accès aux API sans authentification. Les résultats sont préoccupants : près de 19 % des serveurs exposés hébergent des modèles prêts à l'emploi, et les autres peuvent être détournés pour en héberger. Trois pays concentrent la majorité des serveurs vulnérables : les États-Unis (36,6 %), la Chine (22,5 %) et l'Allemagne (8,9 %). Les risques sont multiples : accès non autorisé à l'API, détournement de ressources de calcul, jailbreaking des modèles pour générer du contenu illicite, et possibilité de téléverser des modèles malveillants. Ces serveurs semblent majoritairement être le fruit de tests ou d'expérimentations personnelles, souvent déployés avec des configurations par défaut, sans authentification ni isolation réseau. Cette négligence technique ouvre une surface d'attaque inédite, facilement exploitable. Pour limiter ces menaces, il est essentiel d'adopter des pratiques de base : authentification obligatoire, cloisonnement réseau, configuration sécurisée et surveillance des accès. L'IA locale ne peut se développer durablement sans une attention rigoureuse à la cybersécurité.

Sources

https://www.it-connect.fr/securite-ia-plus-de-1-100-serveurs-ollama-exposes-sur-le-web-sans-authentification/

https://www.lemondeinformatique.fr/actualites/lire-plus-d-un-millier-de-serveurs%02ollama-exposes-sur-internet-97752.html