Злоумышленники получили доступ к тысячам незащищённых моделей искусственного интеллекта.

Исследователи в области безопасности ИИ выявили серьёзную уязвимость в открытой платформе искусственного интеллекта Ollama. Уязвимость, получившая кодовое имя Probllama и идентификационный номер CVE-2024-37032. Проблема могла быть использована злоумышленниками для удалённого выполнения кода.

Недостаток безопасности был выявлен компанией Wiz — это стартап, который предоставляет решения для кибербезопасности облачной инфраструктуры AWS, Microsoft Azure и GCP. Компания была основана в 2020 году бывшими руководителями Microsoft Cloud Security Group." data-html="true" data-original-title="Wiz" >Wiz, занимающейся облачной безопасностью. Проблема была официально раскрыта 5 мая 2024 года и устранена в версии 0.1.34, выпущенной 7 мая 2024 года.

Платформа Ollama предназначена для упаковки, развёртывания и запуска крупных языковых моделей (Большая языковая модель (Large Language Model, LLM) – это глубоко обученная нейронная сеть, используемая для обработки естественного языка. LLM обучается на огромных корпусах текстов и пытается предсказывать следующий токен (слово, знак препинания или другой элемент текста) на основе предыдущих токенов. LLM может использоваться для многих задач обработки текста, таких как генерация текста, перевод, перефразирование, классификация и т.д." data-html="true" data-original-title="LLM" >LLM) на устройствах под управлением Windows, Linux и macOS. Основной проблемой стала недостаточная проверка вводимых данных, что и привело к уязвимости типа Path Traversal (Directory Traversal) представляет собой уязвимость, которая позволяет злоумышленнику получить доступ к файлам и директориям, находящимся за пределами предполагаемой корневой директории веб-сервера.

 Эксплуатация достигается путем манипулирования переменными, которые ссылаются на файлы (например, через URL-запросы), используя специальные последовательности символов, такие как "../" (возвращающиеся на уровень выше в структуре каталогов).

 Таким образом, хакер может обойти ограничения доступа и читать, а иногда и изменять файлы, к которым обычно доступ ограничен. Недостаток позволяет получить несанкционированный доступ к конфиденциальным данным." data-html="true" data-original-title="Path Traversal" >Path Traversal. Эта уязвимость позволяла злоумышленникам перезаписывать произвольные файлы на сервере и выполнять удалённый код.

Для успешной эксплуатации уязвимости злоумышленнику необходимо было отправить специально сформированные HTTP-запросы к API серверу Ollama. В частности,

Все права защищены

save pdf date >>> 06.12.2025

эксплуатировался конечный пункт API «/api/pull», предназначенный для загрузки моделей из официального или частного репозитория. Злоумышленники могли предоставить вредоносный файл манифеста модели, содержащий вредоносный путь в поле digest.

Эта уязвимость могла использоваться для повреждения файлов системы и удалённого выполнения кода путём перезаписи конфигурационного файла «etc/ld.so.preload», связанного с динамическим компоновщиком («ld.so»), для включения вредоносной библиотеки и её запуска перед выполнением любой программы.

Хотя риск удалённого выполнения кода в стандартных установках Linux минимален, в Docker-развёртываниях, где API-сервер открыт для публичного доступа, риск возрастает многократно. В этих условиях сервер работает с правами root и прослушивает 0.0.0.0, что позволяет удалённую эксплуатацию уязвимости.

Исследователь безопасности Саги Цадик отметил, что проблема особенно серьёзна в установках Docker, так как сервер работает с правами суперпользователя и слушает все сетевые интерфейсы.

Дополнительной проблемой является отсутствие аутентификации в Ollama, что позволяет злоумышленникам эксплуатировать общедоступные серверы для кражи или изменения моделей ИИ и компрометации серверов для самоуправляемого вывода ИИ.

Для обеспечения безопасности таких сервисов рекомендуется использовать промежуточное ПО, такое как обратные прокси-серверы с аутентификацией. Wiz выявила более 1000 открытых инстансов Ollama, хранящих множество ИИ-моделей без какой-либо защиты.

Цадик добавил, что CVE-2024-37032 — это легкоэксплуатируемая уязвимость, несмотря на современный код платформы Ollama. «Классические уязвимости, такие как Path Traversal, остаются проблемой даже в новейших программных продуктах».

Компания Protect AI также недавно предупреждала о более чем 60 уязвимостях в различных инструментах для ИИ/ML, включая критические проблемы, такие как раскрытие информации, доступ к ограниченным ресурсам, повышение привилегий и полный захват системы. Самая серьёзная из этих уязвимостей, CVE-2024-22476, представляет собой SQL-инъекцию в программном обеспечении Intel Neural Compressor, что позволяет злоумышленникам загружать произвольные файлы с хост-системы.

Все права защищены

save pdf date >>> 06.12.2025