В расширении Amazon Q для Visual Studio Code обнаружили вредоносный код. Это бесплатный ИИ-инструмент, который помогает программистам писать и отлаживать код. Он был загружен почти миллион раз.

13 июля хакер под псевдонимом lkmanka58 добавил в репозиторий проекта на GitHub опасный код, который должен был удалять файлы и облачные ресурсы, имитируя «сброс до заводских настроек». Вреда он не причинил — скорее это была демонстрация уязвимости.

Хакер получил доступ, вероятно, из-за ошибки в настройке прав доступа. Amazon не заметил проблему и опубликовал заражённую версию расширения (1.84.0) 17 июля. Только 23 июля компания получила сообщение от исследователей безопасности и начала расследование.

На следующий день вышла обновлённая безопасная версия — 1.85.0. В Amazon утверждают, что вредоносный код был написан с ошибками и не мог выполниться. Однако некоторые специалисты уверены, что он запускался, хоть и не нанёс ущерба.