В новой программе Google Gemini CLI обнаружили серьёзную уязвимость, которая могла позволить злоумышленникам запускать вредоносные команды на компьютерах разработчиков без их ведома.

Gemini CLI — это инструмент, который позволяет программистам общаться с искусственным интеллектом Google прямо через командную строку. Он может читать код, давать советы и запускать команды на устройстве пользователя.

Проблема заключалась в том, что Gemini автоматически выполнял команды из списка доверенных. Хакеры могли спрятать вредоносные инструкции рядом с обычными командами в файлах, которые Gemini читает, например, в README.md. Так вредоносный код мог украсть личные данные или установить скрытый доступ.

Пользователь при этом не получал никаких предупреждений, так как Gemini считал команды безопасными. Злоумышленники могли использовать хитрую маскировку, чтобы скрыть вредоносные команды от глаз пользователя.

Google уже выпустила обновление Gemini CLI версии 0.1.14, в котором эта ошибка исправлена.