Исследователи рекомендуют немедленно удалить популярное браузерное расширение.

Специалисты из Cybersecurity Research Center (CyRC) компании Synopsys обнаружили zero-day уязвимость в EmailGPT, популярном расширении для Google Chrome, использующем искусственный интеллект для написания электронных писем.

Уязвимость типа «Prompt Injection» с идентификатором CVE-2024-5184 позволяет злоумышленникам манипулировать сервисом и получать доступ к конфиденциальной информации.

EmailGPT использует общедоступные ИИ-модели от OpenAI для помощи пользователям в составлении писем в сервисе Gmail — это бесплатная почтовая служба, предоставляемая компанией Google. Она позволяет пользователям создавать и управлять своими электронными письмами. Gmail предлагает множество функций, включая большой объем хранилища, удобный интерфейс, организацию писем в различные папки и эффективную систему фильтрации спама. Также в Gmail доступны календарь, задачи, контакты и многое другое." data-html="true" data-original-title="Gmail" >Gmail. Пользователи получают ИИ-подсказки для написания писем, предоставляя сервису исходные данные и контекст. Однако недавнее открытие выявило серьёзный изъян в работе расширения.

EmailGPT использует API-сервис, который позволяет злоумышленникам внедрять сторонние промпты и управлять логикой сервиса. Это может привести к утечке системных подсказок или выполнению нежелательных команд.

Так, злоумышленник может создать промпт, который встраивает нежелательную функциональность, что может привести к:

Эта уязвимость, оцененная в 6.5 балла по шкале CVSS, может также привести к утечке интеллектуальной собственности, отказу в обслуживании и финансовым потерям.

Synopsys сообщает, что их исследователи связались с разработчиками EmailGPT до публикации деталей, но ответа не получили. Synopsys рекомендует немедленно удалить EmailGPT из своего браузера, ведь каких-либо путей для смягчения последствий уязвимости пока нет.

Пользователям рекомендуется следить за обновлениями и патчами для обеспечения безопасности. По мере развития ИИ-технологий важность бдительности и надёжных мер безопасности возрастает.

Патрик Харр, CEO компании SlashNext Email Security, отметил важность строгого управления и внедрения дополнительных мер безопасности для ИИ-моделей, чтобы предотвратить появление уязвимостей и их последующую эксплуатацию.

Харр также добавил, что компании, планирующие интеграцию ИИ в свои бизнес-процессы, должны требовать от поставщиков ИИ-моделей реальных доказательств их безопасности.