Американское агентство по кибербезопасности (CISA) предупредило об активной эксплуатации уязвимости в платформе Langflow, популярном инструменте для создания ИИ-приложений. Уязвимость, известная как CVE-2025−3248, позволяет хакерам без авторизации выполнять произвольный код на серверах, получая полный контроль над системой. Об этом сообщает BleepingComputer.

Langflow — это открытая платформа для визуального создания рабочих процессов на основе искусственного интеллекта. Уязвимость связана с ошибкой в API, которая позволяет злоумышленникам отправлять вредоносные запросы. По данным СМИ, на данный момент 466 серверов Langflow доступны в интернете, что делает их потенциальными целями. Проблема затрагивает все версии до 1.3.0, новая версия 1.4.0 уже содержит исправления.

CISA добавила уязвимость в список активно эксплуатируемых угроз, требуя от федеральных агентств обновить ПО до 26 мая. Исследователи из Horizon3 отметили, что уязвимость легко использовать из-за слабой защиты платформы.

Организациям, использующим Langflow, срочно рекомендуется обновиться до версии 1.4.0 и ограничить доступ к серверам из интернета.