Исследователи из Microsoft Threat Intelligence обнаружили способ обойти систему защиты Transparency, Consent, and Control (TCC) в macOS.

Уязвимость получила название Sploitlight и позволяла получать доступ к конфиденциальным данным пользователя без его ведома.

Речь идет о таких данных, как координаты геолокации, метаданные фотографий и видео, история поиска, настройки пользователя, а также ИИ-сводки писем и информация из медиатеки с распознаванием лиц.

По данным Microsoft, проблема заключалась в том, что Spotlight-плагины, предназначенные для отображения данных приложений в поиске, можно было модифицировать таким образом, чтобы они утекали за пределы изолированной среды, установленной Apple.

Исследователям удалось подменить содержимое некоторых файлов, и Spotlight, не заметив подмены, начал кэшировать и передавать данные, которые должны были оставаться закрытыми.

Компания своевременно сообщила об уязвимости Apple. Та закрыла дыру в обновлениях macOS 15.4 и iOS 15.4, выпущенных 31 марта 2025 года.

В Microsoft подчеркивают, что уязвимость не использовалась злоумышленниками на практике.

Apple же в своем отчете указала, что устранение проблемы было достигнуто за счёт улучшенного скрытия данных, а также подтвердила, что одновременно были закрыты ещё две уязвимости, также найденные Microsoft.