Ранее мы сообщали о новой функции Microsoft Recall для Windows 11, работающей на базе искусственного интеллекта на компьютерах Copilot+. Эта функция постоянно делает скриншоты ваших действий. Объявление об этом обновлении на конференции Build вызвало обеспокоенность по поводу безопасности. Несмотря на заверения Microsoft о шифровании данных и соблюдении конфиденциальности, исследователь безопасности назвал эту функцию "катастрофой" для безопасности

Хотя Microsoft утверждает, что функция Recall зашифрована, эксперт по кибербезопасности Кевин Бомонт выразил сомнения в этом. При тестировании он обнаружил, что данные хранятся в базе данных в виде обычного текста. Это вызвало у него серьёзные опасения по поводу плохо реализованной функции, которая может негативно повлиять на репутацию компании и её клиентов.

Бомонт сообщил, что пользовательские данные сохраняются в виде обычного текста в базе данных SQLite, содержащей записи о всех действиях на ПК. Поскольку данные хранятся в пользовательской папке, к ним могут получить доступ хакеры через вредоносное ПО. Он предупредил, что эта функция может предоставить киберпреступникам больше возможностей для атак и привести к "супервзлому с использованием искусственного интеллекта"

Microsoft заявляет, что данные защищены, так как хранятся локально и зашифрованы, но Бомонт утверждает, что доступ к базе данных возможен даже без административных прав, через файлы AppData. Он продемонстрировал это, извлекая данные и создавая веб-сайт для загрузки базы данных, где можно было искать информацию в файлах.

Бомонт пока не раскрыл технические детали процесса взлома, ожидая реакции Microsoft. Он считает, что из-за возможных проблем безопасности лучше временно приостановить развертывание этой функции. Microsoft пока не ответила на эти проблемы, но функция Recall является опциональной и может быть отключена, если пользователи не хотят её использовать. Выпуск ПК Copilot+ с функцией Recall запланирован на 18 июня.