Протокол удаленного рабочего стола (RDP) в Windows позволяет входить в систему с использованием старых, уже измененных паролей, и Microsoft называет это не уязвимостью, а частью спецификации. Об этом сообщает Tweakers со ссылкой на исследование специалиста по безопасности Кевина Бомонта.

Проблема заключается в функции Windows, которая сохраняет до 10 предыдущих паролей в виде хэшей — зашифрованных данных, используемых для проверки подлинности. Даже после смены пароля старые хэши остаются активными для входа через RDP.

Бомонт утверждает, что это создает потенциальный «вечный бэкдор», позволяя злоумышленникам, знающим старый пароль, получить доступ к системе. Microsoft, однако, настаивает, что это осознанное решение для удобства пользователей, и рекомендует отключать кэширование паролей или использовать двухфакторную аутентификацию (2FA) для повышения безопасности. 2FA требует дополнительного подтверждения, например, кода с телефона, что якобы снижает риски.

Эксперты отмечают, что проблема актуальна для организаций, где сотрудники могут случайно или намеренно раскрывать старые пароли. Хотя Microsoft не планирует устранять эту особенность, компании могут минимизировать угрозы, регулярно обновляя политики безопасности и отключая устаревшие протоколы.