Автор: Administrator
22.07.2021 13:36

{jcomments on}

Исследователь в области информационной безопасности Jonas Lykkegaard сообщил об опасной уязвимости CVE-2021-36934, которая затрагивает операционные системы Windows 10 и Windows 11. Эксплуатация проблемы, получившей названия SeriousSAM и HiveNightmare, позволяет локальному пользователю повысить свои привилегии и получить доступ к конфиденциальным файлам базы данных реестра.

Реестр операционной системы Windows действует как база данных конфигураций и содержит хеши паролей, пользовательские настройки, параметры конфигурации для приложений, ключи дешифрования системы и пр.

Файлы базы данных, связанные с реестром Windows, хранятся в каталоге C:Windowssystem32config и разбиты на разные файлы, такие как **SYSTEM, SECURITY, SAM, DEFAULT и SOFTWARE**
. Поскольку эти файлы содержат конфиденциальную информацию обо всех учетных записях пользователей на устройстве и токенах безопасности, используемых функциями Windows, они запрещены для просмотра обычными пользователями без повышенных прав.

Это особенно важно для файла диспетчера учетных записей безопасности (Security Account Manager, SAM), поскольку он содержит хеши паролей для всех пользователей в системе, которые злоумышленники могут использовать для подтверждения своей личности.

По словам Jonas Lykkegaard, файлы реестра Windows 10 и Windows 11, связанные с SAM и всеми другими базами данных реестра, доступны для группы «Пользователи» с

низкими привилегиями на устройстве. Во время тестирования Windows 11 специалист обнаружил, что хотя ОС ограничивает доступ к этим файлам для низкоуровневых пользователей, доступные копии файлов сохраняются в теневых копиях. Данная проблема появилась в коде Windows 10 еще в 2018 году, после выпуска версии 1809.

В качестве временных мер по предотвращению эксплуатации уязвимости специалисты компании Microsoft рекомендуют ограничить доступ к уязвимой папке, а также удалить теневые копии.

Источник: www.securitylab.ru