Уязвимость системы безопасности DPAPI Windows 10

Passcape Software

1 Уязвимость системы безопасности DPAPI Windows 10

1.1 Краткое описание

Наши специалисты нашли новую серьезную брешь в системе безопасности DPAPI, позволяющую расшифровать персональные данные последнего активного пользователя Windows 10.

1.2 Какие ОС затрагивает

Уязвимости подвержены все версии Windows 10, начиная с 1709 (Fall Creators Update), а также учетные записи Microsoft в предыдущих версиях Windows 10, если включена функция шифрования системного диска.

1.3 Что такое DPAPI

Data Protection Application Programming Interface или сокращенно DPAPI - является основным механизмом защиты персональных данных пользователя во всех операционных системах Windows, начиная с Windows 2000. DPAPI стала популярной в первую очередь из-за простоты использования, поскольку состоит всего лишь из двух функций шифрования и расшифровки конфиденциальных данных: CryptProtectData и CryptUnprotectData. Но несмотря на кажущуюся простоту, внутренний механизм работы CryptProtectData/CryptUnprotectData довольно сложный. Подробнее о логике работы DPAPI можно почитать в нашей статье.

1.4 Предыдущие уязвимости DPAPI

DPAPI была создана с учетом многих аспектов безопасности и по-праву может считаться одной из лучших систем защиты данных, являясь наглядных примером того, как изначально хорошо продуманный продукт может служить долгие годы. Однако, первая реализация DPAPI имела очень серьезную проблему, благодаря которой вся защита сводилась к нулю. Дело в том, что основной ключ шифрования DPAPI формировался на основе NTLM хэша пароля пользователя. Это означало, что достаточно было получить доступ к NTLM хэшу, который хранился в реестре SAM, чтобы расшифровать все пароли DPAPI. К счастью, в Microsoft быстро обнаружили просчет в логике и выкатили вторую, исправленную версию DPAPI, которая работает и по сей день.

Новая уязвимость в чем-то похоже на первую проблему, за исключением следующих пунктов:

- Новая проблема DPAPI затрагивает лишь последнего активного пользователя системы.
- Новая уязвимость не распространяется на доменные учетные записи.
- В отличие от первой реализации DPAPI, новая уязвимость это не ошибка разработчиков, а вынужденный компромисс безопасности и удобства работы, если можно так выразиться.

1.5 Что такое Automatic Restart Sign-On (ARSO)

Начиная с Windows 8 появилась возможность запуска приложений экрана блокировки. То есть приложений, запускающих и отображающих уведомления, пока сеанс пользователя заблокирован. Например, встречи календаря, уведомления электронной почты, сообщений и т.д. Однако, во время автоматической перезагрузки системы после обновления, эти приложения перестали бы работать, поскольку для их работы требуется активная сессия пользователя. Возникает очевидный конфликт безопасности, который был решен Microsoft довольно оригинальным способом.

Перед тем, как система обновлений начнет автоматическую перезагрузку, текущие учетные данные пользователя сохраняются в специальном секрете LSA. После перезагрузки эти учетные данные используются для автоматического входа пользователя в систему и создания активной сессии, но при этом интерактивная часть будет недоступна пользователю до тех пор, пока он не введет пароль, ПИН-код и т.д. Таким образом, последняя сессия пользователя будет автоматически восстановлена, приложения экрана блокировки могут работать. Так работает система Automatic Restart Sign-On.

1.6 Что такое Trusted Boot Auto-Logon (TBAL)

В Windows 10 система ARSO использует механизм Trusted Boot Auto-Logon (TBAL). Надо сказать, возможность автоматического входа пользователя в систему без ввода пароля присутствует во всех версиях Windows. Для этого в реестре Windows необходимо изменить опцию для автоматического входа и прописать текстовый пароль на вход. При загрузке система видит эту опцию, читает ее и использует сохраненный пароль для автоматического входа.

В Windows 10 автоматический вход в систему был дополнен механизмом TBAL. TBAL является своего рода симбиозом обычного автоматического входа и ARSO. Но имеет и ряд отличий, главные из которых это:

- Поддержка учетных записей Microsoft
- Отказ от хранения пароля в текстовом виде
- TBAL включен всегда, а не только тогда, когда требуется автоматическая перезагрузка. На первых версиях Windows 10, TBAL активировался только после включения шифрования системного диска.

Каков же механизм работы TBAL?

1.7 Как работает TBAL

В Windows 10 перед завершением работы система записывает в LSA секрет с именем **DefaulPassword** специальный пароль *_TBAL_{68EDDCF5-0AEB-4C28-A770-AF5302ECA3C9}*, признак того, что хранится не обычный пароль автоматического входа, а маркер TBAL. Далее, в зависимости от типа последней активной учетной записи, создается еще один LSA секрет для локального или облачного провайдера. Если это обычная учетная запись, то создается секрет с именем **M$_MSV1_0_TBAL_PRIMARY_{22BE8E5B-58B3-4A87-BA71-41B0ECF3A9EA**, в который записывается имя пользователя, NTLM и SHA1 хэши пароля, а также другая служебная информация. Если это учетная запись Microsoft, то создается секрет с именем **M$_CLOUDAP_TBAL_{8283D8D4-55B6-466F-B7D7-17A1352D9CAB}_<UID>** (Windows 1607 и ранее) или **M$_CLOUDAP_TBAL_{4416F0BD-3A59-4590-9579-DA6E08AF19B3}_<UID>**, где **<UID>** это SHA256 хэш универсального идентификатора пользователя. Этот секрет содержит 96-байтный ключ, нужный для расшифровки основного ключа шифрования DPAPI.

После перезагрузки система определяет маркер TBAL и расшифровывает основной ключ шифрования DPAPI при помощи либо SHA1 хэша (для оффлайн учетной записи), либо 96-байтного ключа, если это учетная запись Microsoft. После этого оба LSA-секрета удаляются. TBAL маркер не записывается во время гибернации или завершении активной сессии пользователя, только перед перезагрузкой или завершением работы компьютера.

1.8 Причина уязвимости

Уязвимость заключается в том, что после завершения работы системы, любой, кто имеет физический доступ к ПК, может использовать сохраненный секрет TBAL для расшифровки первичного ключа шифрования DPAPI и, как следствие, всех данных пользователя, которые зашифрованы при помощи DPAPI. Очевидно, что причина уязвимости, в отличие от первой версии DPAPI или от предыдущих ошибок в реализации безпарольного входа, состоит не в ошибочной логике работы, а в концептуальном подходе Microsoft к обеспечению безопасности Windows. Впрочем, это глобальный тренд последних лет.

1.9 Какие данные в опасности

- Сетевые пароли, хранящиеся в некоторых популярных интернет обозревателях: Google Chrome, Internet Explorer, Microsoft Edge, Opera и др.
- Пароли почтовых клиентов Microsoft Office Outlook, Windows Mail
- Пароли доступа к общим папкам и ресурсам
- Пароли и ключи шифрования, хранимые в Windows Vault
- Пароли соединений удаленного доступа к рабочему столу
- Приватные ключи Системы Шифрования Файлов (EFS)
- Ключи шифрования почты S-MIME
- Сертификаты пользователя
- Сетевые пароли, хранимые в Credential Manager
- Персональные данные любого приложения, программно защищенные при помощи DPAPI. Например, Skype, Windows Rights Management Services, Windows Media, Google Talk и т.д.

1.10 PoC

Это видео демонстрирует, насколько просто получить доступ к персональным данным последнего пользователя системы, не зная его пароля на вход. Пароль Facebook, хранящийся в Windows Vault, расшифровывается автоматически. Хотя система DPAPI предполагает, что без знания пароля пользователя на вход, этого сделать нельзя.

1.11 Выводы

Как мы и говорили в нашей предыдущей статье, следующие версии Windows будут становиться все менее и менее ориентированы на обеспечение сохранности приватных данных. Тем пользователям, для которых важен максимальный уровень защиты своих персональных данных, рекомендуется использовать оффлайн учетные записи и Windows 10 до версии 1709 с включенным SYSKEY-паролем или полным шифрованием системного диска.