Аннотация – в документе представлен анализ уязвимостей в решения класса Mobile Device Management (MDM). Анализ охватывает различные аспекты этих уязвимостей, включая их технические детали, потенциальные векторы атак и последствия для специалистов по безопасности и организаций в различных отраслях.

Анализ предоставляет высококачественную сводную информацию об этих уязвимостях, предлагая ценную информацию специалистам по безопасности, ИТ-администраторам и другим специалистам. Понимая эти уязвимости и их последствия, организации могут лучше защищать свои решения MDM, повышать уровень безопасности и снижать риски, связанные с этими недостатками. Этот документ служит важным ресурсом для тех, кто хочет защитить свои системы управления мобильными устройствами от сложных киберугроз.

I. MobileIron MDM

Уязвимость системы безопасности в решении MobileIron MDM подвергает user enumeration и однофакторную аутентификацию (SFA) атакам без проверки подлинности. Анализ показывает, что статический ключ в MobileIron MDM может использоваться для получения списка учётных записей пользователей, что потенциально приводит к несанкционированному доступу.

A. Закодированный ключ шифрования Mobile@Work:

Агент Mobile@Work использует закодированный ключ API, который может быть извлечён злоумышленником, не прошедшим проверку подлинности, для обнаружения конечной точки аутентификации MobileIron организации.

- Агент Mobile@Work использует закодированный ключ шифрования для процесса аутентификации, который может позволить злоумышленнику создавать запросы аутентификации MobileIron и потенциально перехватывать учётные данные учётной записи с помощью атак типа "человек посередине" (MitM).
- MobileIron признает эту проблему, но считает вектор атаки минимальным из-за многоуровневой стратегии шифрования через TLS.

1) Реакция MobileIron на проблемы безопасности:

- MobileIron рекомендует настраивать свои основные продукты с использованием многофакторной аутентификации и взаимной аутентификации по сертификатам для обеспечения безопасности регистрации устройств.
- Они опровергают несколько выводов из отчёта Optiv, предполагающих, что тестируемый сервер MobileIron Core не был настроен должным образом.

2) CVE-2021-3391:

- Эта уязвимость позволяет злоумышленникам различать действительные, отключённые и несуществующие учётные записи пользователей по количеству неудачных попыток входа, необходимых для выдачи сообщения об ошибке блокировки.

3) Общие методы обеспечения безопасности и уязвимости:

- Hardcode ключей доступа в мобильных приложениях / API не считается безопасным, поскольку все, что встроено в клиент, полностью доступно пользователям, что позволяет воспроизвести любой запрос приложения.
- Использование закодированных ключей является распространённой уязвимостью, позволяющей расшифровывать зашифрованные файлы конфигурации и извлекать конфиденциальную информацию.

4) Безопасность платформы MobileIron:

- Платформа MobileIron обеспечивает функции безопасности, такие как аудит безопасности, криптографическая поддержка, идентификация и аутентификация, управление безопасностью и защита TSF.
- Он использует TLS для защиты каналов связи между собой и пользователями мобильных устройств.

5) CVE-2020-35138:

- MobileIron agents для Android и iOS содержат заданный ключ шифрования, используемый для шифрования данных имени пользователя / пароля в процессе аутентификации.

6) Статический ключ MobileIron MDM для получения списка учётных записей:

- Hardcode ключ API в Mobile@Work agent позволяет получить список учётных записей, демонстрируя уязвимость в системе безопасности.

7) Уязвимости в системе безопасности MobileIron:

- В MobileIron agents для Android и iOS были выявлены различные уязвимости в системе

безопасности, включая использование закодированного ключа API и ключа шифрования.

8) *Уязвимость MobileIron CVE2020-15505:*
- Эта уязвимость была использована группами APT-национальных государств и киберпреступниками для компрометации организаций.

9) *Правительство Норвегии взломали с помощью:*
- Правительство Норвегии было взломано с использованием 0day-уязвимости MobileIron, что подчёркивает важность защиты среды MobileIron от известных уязвимостей.

B. Hardcode ключ API для мобильных устройств@Work

Агент Mobile@Work использует закодированный ключ шифрования, позволяющий злоумышленнику, не прошедшему проверку подлинности, создавать запросы аутентификации MobileIron. Это также может позволить злоумышленнику перехватить учётные данные с помощью атак типа "человек посередине" (MitM).

1) *Процесс регистрации MobileIron MDM:*
- Пользователи запускают приложение Mobile@Work и указывают свой адрес электронной почты или конечную точку среды MobileIron MDM.
- Отправка электронного письма инициирует discovery-процесс с помощью API, размещенного на MobileIron, для идентификации конечной точки аутентификации.

2) *Discovery-запрос API:*
- Для запроса API требуются два значения:
  - ключ API MobileIron для авторизации запросов.
  - зарегистрированное ПОЛНОЕ доменное имя адреса электронной почты пользователя.
- Запросы без валидного ключа API выдают ошибку HTTP 403.

3) *Hardcode ключ API в Mobile@Work Agent:*
- Ключ API MobileIron закодирован в приложении Mobile@Work agent.
- Декомпиляция файла Android APK, чтобы получить исходный код Java.
- В файле был найден закодированный ключ API. sources/com/mobileiron/registration/RegisterActivity.java

4) *Влияние закодированного ключа:*
- Восстановление этого ключа API позволяет любому злоумышленнику, не прошедшему проверку подлинности, найти конечную точку аутентификации MobileIron организации.
- Запрос на успешное обнаружение API с использованием закодированного ключа.

5) *Ответ MobileIron:*
- MobileIron признал проблему и определил как критически важную для рабочего процесса Mobile @Work.
- Они рассматривают альтернативные решения, но в настоящее время нет сроков для исправления.
- Проверка CVE-2020–35137 может быть выполнена с помощью инструмента под названием Dauthi

C. Получение списка учётных записей в MobileIron

Процесс аутентификации учётной записи позволяет внешним организациям получать учётные записи пользователей и выполнять атаки с целью аутентификации без запуска условий блокировки учётной записи. Организации могут отслеживать конечную точку MobileIron на предмет чрезмерных запросов аутентификации, чтобы получать информацию о вредоносной активности.

1) *Интеграция с Active Directory (AD):*
- MobileIron обычно интегрируется Microsoft Active Directory (AD), используя LDAP для просмотра пользовательского хранилища.
- Регистрация устройств разрешена не для всех видимых пользователей по умолчанию; учётные записи должны быть включены в MobileIron, прежде чем будет разрешена регистрация устройств.

2) *Ответы на проверку подлинности:*

MobileIron предоставляет различные ответы на основе содержимого протокола MobileIron (MIPR):
- **Успешная аутентификация**: результатом является сжатая полезная нагрузка zLib, содержащая профиль MobileIron MDM с такими данными, как имя пользователя, SenderGUID, UUID и значение файла cookie.
- **Сбой аутентификации**: идентифицирован, по определённому сообщению, 0x1D.
- **Блокировка учётной записи**: срабатывает после порогового значения неудачных попыток с продолжительностью блокировки около 30 секунд.

3) *Вспомогательные ответы:*
- **Null Response**: указывает на проблему с форматом или условным вводом.
- **Device Unregistered**: указывает на аннулированный или незарегистрированный сеанс авторизации по PIN-коду.
- **Unknown Client ID**: указывает недопустимый или неизвестный идентификатор отправителя.

4) *Интересные элементы в пакете подготовки:*
- **cookie**: представляет аутентифицированный и зарегистрированный сеанс MDM.
- **easV3Signature**: сертификат в кодировке Base64 для взаимной аутентификации по сертификатам.

- **easi**: заголовок авторизации HTTP-клиента.
- **rsn**: значение UUID устройства, используемое в качестве первичного ключа для регистрации MDM.
- **senderGUID**: числовой идентификатор для прошедшего проверку подлинности и зарегистрированного сеанса MDM.
- **userID / username**: указывает имя пользователя, связанное с сеансом аутентификации.

5) Сбой аутентификации и блокировка:

- Порог блокировки MobileIron составляет около пяти неудачных попыток, что является локальным условием и не влияет на вышестоящий AD.
- Событие блокировки обозначается конкретным ответом 0x1D.

6) UserEnumeration:

- **Недействительная учётная запись**: условие блокировки не выполняется, что указывает на недопустимость имени пользователя.
- **Отключённый / заблокированный AD аккаунт**: первая попытка завершается неудачей, а вторая попытка приводит к ответу о блокировке.
- **Действительная учётная запись**: пять неудачных попыток, прежде чем возникнет условие блокировки.
- Проверка CVE-2021–3391 может быть выполнена с помощью инструмента под названием Dauthi.

D. Стратегии смягчения последствий

1) Аутентификация на основе PIN-кода

- Для аутентификации по PIN-коду может использоваться одно значение PIN-кода или PIN-код + учётные данные пользователя.
- ПИН-коды — это 6-значные одноразовые значения, привязанные к одному аккаунту.
- Однако запросы на аутентификацию PIN-кода не регулируются, что позволяет принудительно использовать действительные PIN-коды.
- Регистрация на основе PIN-кода предотвращает использование метода user enumeration
- Таким образом, аутентификация на основе PIN-кода успешно снижает вероятность атаки MobileIron.

2) Взаимная аутентификация по сертификатам

- Это позволяет проверять достоверность TLS только агента Mobile@Work agent.
- Исходя из этого, взаимная аутентификация по сертификатам не смягчает поверхность атаки.

3) Дополнительные рекомендации

- **Политика надёжных корпоративных паролей**:
  - Внедрение политику минимальной длины пароля в 12 символов.
  - Объединение с блокирующими списками распространённые шаблоны паролей.
- **Ограничение регистрации пользовательского устройства**:
  - Разрешает только один UUID и / или подтверждённые значения UUID для регистрации устройства.
  - Предотвращает регистрацию устройства со скомпрометированной учётной записью.
- **Отслеживание запросы на аутентификацию MDM**:
  - Отслеживание службы MobileIron connector и регистрируйте вредоносную активность.
  - Поиск bruteforce попыток аутентификации.