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. FileWave MDM

FileWave MDM — комплексное многоплатформенное решение для управления мобильными устройствами, которое позволяет ИТ-администраторам управлять устройствами организации, отслеживать их и обеспечивать их безопасность. Он поддерживает широкий спектр устройств, включая смартфоны с iOS и Android, планшеты macOS и Windows, ноутбуки, рабочие станции и интеллектуальные устройства, такие как телевизоры.

FileWave MDM предлагает централизованное управление устройствами, позволяя администраторам отслеживать их и управлять ими из единого интерфейса. Он включает в себя несколько функций безопасности, таких как шифрование данных, возможности удалённой очистки и политики паролей, которые помогают защитить устройства и данные от несанкционированного доступа. Платформа может быть настроена в соответствии с конкретными потребностями организации, что позволяет администраторам настраивать параметры и политики по мере необходимости. Кроме того, FileWave MDM позволяет автоматизировать многие задачи, такие как обновление программного обеспечения и конфигурирование устройств, экономя время и снижая риск ошибок. Он совместим с широким спектром устройств и операционных систем, включая macOS, Windows, iOS, iPadOS, tvOS, ChromeOS и Android

A. Проблемы аутентификации

1) Выявленные уязвимости:

- Две уязвимости, CVE-2022–34907 и CVE-2022–34906, были обнаружены в системе управления мобильными устройствами (MDM) FileWave.
- CVE-2022-34907 — уязвимость, которая позволяет злоумышленникам получить доступ от имени учётных записей обходя аутентификацию.
- CVE-2022-34906 сфокусирована на закодированном криптографическом ключе, который может быть использован для получения несанкционированного доступа.

2) Влияние уязвимостей:

- Эти уязвимости можно использовать удалённо, позволяя обойти механизмы аутентификации и получить полный контроль над платформой MDM и управляемыми ею устройствами.
- Злоумышленники получают доступ к конфиденциальным данным: адреса электронной почты пользователей, серийные номера устройств, полные имена, адреса, географические координаты, IP-адреса и PIN-коды устройств.
- Можно использовать MDM для установки вредоносных пакетов или исполняемых файлов и получения прямого доступа к устройствам через протоколы удалённого управления.

3) Объем уязвимостей:

- В различных отраслях промышленности, включая правительственные учреждения, образовательные учреждения и крупные предприятия, было выявлено более 1100 уязвимых FileWave.
- Каждый уязвимый экземпляр содержал неограниченное количество управляемых устройств, что делало их главными целями для потенциальных атак.

4) Реализация:

- Выполняется стандартная установка FileWave и регистрируется шесть устройств для демонстрации уязвимости.
- Используя уязвимость обхода аутентификации, можно получить полный контроль над экземпляром MDM, получить данные и установить вредоносные пакеты, включая поддельный вирус-вымогатель.

5) Смягчение последствий и ответные меры:

- FileWave устранила эти уязвимости в версии 14.7.2 и призвала пользователей применить обновление для снижения рисков.
- Компания активно работала с клиентами, чтобы гарантировать, что затронутые системы будут исправлены или обновлены.

- Пользователям рекомендуется дважды проверить правильность установки и актуальность обновления для системы безопасности, чтобы избежать риска атак сторонних производителей.

6) Меры безопасности:

- FileWave шифрует весь пользовательский контент при передаче и в состоянии покоя.
- Платформа поддерживает широкий спектр устройств, включая смартфоны iOS и Android, планшеты macOS и Windows, ноутбуки, рабочие станции и интеллектуальные устройства, такие как телевизоры.
- Веб-сервер MDM (Python/Django), обрабатывает регистрацию устройств, извлекает информацию об устройстве и передаёт команды устройствам.

B. Технические детали

Ключевая уязвимость заключается в том, что закодированный секрет планировщика принимается для аутентификации вместо надлежащих учётных данных администратора. Изменения кода в более новых версиях пытались исправить это, но был введён новый обходной вектор с использованием заголовка Host.

- Уязвимость существует в компоненте веб-сервера FileWave MDM, написанном на Python с использованием фреймворка Django. Он предоставляет доступ к TCP-портам 20443 и 20445.
- Веб-сервер обрабатывает регистрацию клиентского устройства, извлекает информацию об устройстве и передает команды устройствам.
- Для клиентских устройств регистрация по умолчанию не требует аутентификации, хотя учётные данные могут быть включены.
- Для аутентификации администратора комбинация имени пользователя и пароля возвращает действительный токен для управляющих устройств.
- Служба внутреннего планировщика использует закодированный общий секрет для аутентификации на веб-сервере вместо учётных данных администратора.
- В более старых версиях (до 13.1.3) предоставление закодированного секрета планировщика в заголовке авторизации предоставляло бы привилегии суперпользователя в обход аутентификации.
- В более новых версиях FileWave добавила проверку на уровне middleware, сравнивающую заголовок авторизации с секретом планировщика и проверяющую, является ли заголовок Host localhost.
- Установив в заголовке Host значение localhost, злоумышленник может обойти новую проверку промежуточного программного обеспечения и получить привилегии суперпользователя.
- Использование уязвимости обеспечивает полный контроль над экземпляром MDM, позволяя злоумышленникам контролировать управляемые устройства, извлекать конфиденциальные данные: пользователей, электронные письма, местоположения, и устанавливать вредоносное ПО.

C. Атака

1) Настройка и первоначальная эксплуатация:

- Стандартная настройка FileWave, с регистрацией шести устройств с различными ОС.
- Веб-сервер MDM с использованием обнаруженной уязвимости, позволяющей осуществить утечку данных обо всех управляемых устройствах.

2) Использование уязвимости обхода аутентификации

- Идентификация Django-компонента веб-сервера MDM, предоставляющего доступ к TCP-портам 20443 и 20445.
- Для более старых версий (до 13.1.3) в заголовке авторизации был указан закодированный секрет планировщика для получения доступа super_user в обход аутентификации.
- Для более новых версий – заголовок Host равным localhost и секрет планировщика в заголовке авторизации, чтобы обойти проверку промежуточного программного обеспечения и получить доступ access

3) Эксфильтрация данных:

- Административный доступ в обход аутентификации на сервере MDM.
- Информация об управляемых устройствах, включая их операционные системы, экосистемы и настройки, была удалена.

4) Установка вредоносного пакета:

- Для установки пакетов и программного обеспечения на управляемые устройства использовалась обычная функциональность MDM.
- На каждом контролируемом устройстве были установлены вредоносные пакеты, включая поддельный вирус-вымогатель.
- злоумышленник может использовать возможности FileWave для получения контроля над различными управляемыми устройствами и выполнения удалённого кода.

5) Демонстрация потенциального вреда:

Эксплойт продемонстрировал серьёзность и потенциальный вред, продемонстрировав способность контролировать все управляемые устройства, удалять конфиденциальные данные и устанавливать вредоносное программное обеспечение.

D. Сценарий эксплуатации CVE-2022-34906

В этом примере показано, как злоумышленник, не прошедший проверку подлинности, может использовать уязвимость с закодированным секретом в FileWave MDM для получения несанкционированного доступа, удаления конфиденциальных данных и потенциальной компрометации управляемых устройств.

1) Определение уязвимости

- FileWave в версиях MDM до 14.6.3 и 14.7.x до 14.7.2 использовался закодированный криптографический ключ.

- Закодированный ключ не менялся между различными установками или версиями файловой MDM-системы.

2) Использование закодированного ключа

- Злоумышленник, не прошедший проверку подлинности, может использовать закодированный ключ для расшифровки информации, хранящейся в файловой системе MDM.
- Злоумышленник также потенциально может отправлять обработанные запросы на устройства, управляемые платформой MDM, злоупотребляя возможностями MDM.

3) Получение несанкционированного доступа

- Используя уязвимость с закодированным ключом, злоумышленник получает несанкционированный доступ к платформе MDM и управляемым ею устройствам.
- Это может позволить злоумышленнику получить конфиденциальные данные с управляемых устройств, включая имена пользователей, адреса электронной почты, IP-адреса, географическое расположение и многое другое.
- Кроме того, злоумышленник потенциально может установить вредоносное программное обеспечение или выполнить произвольный код на управляемых устройствах, злоупотребляя возможностями MDM

E. Сценарий эксплуатации CVE-2022-34907

Для CVE-2022–34907, уязвимости обхода аутентификации в FileWave MDM, процесс технического использования выглядит следующим образом:

1) Подготовка атаки

- Злоумышленник идентифицирует целевой MDM-сервер FileWave, доступный через Интернет.
- Злоумышленник собирает информацию о сервере MDM, такую как его версия, чтобы подтвердить, что он уязвим для CVE-2022–34907.

2) Создание эксплойта

- Злоумышленник отправляет вредоносный HTTP-запрос, предназначенный для веб-сервера FileWave MDM.
- Для версий до 13.1.3 злоумышленник включает закодированный секрет планировщика в заголовок авторизации запроса.
- Для версий новее 13.1.3 злоумышленник изменяет заголовок Host на "localhost" и включает закодированный секрет планировщика в заголовок авторизации.

3) Получение несанкционированного доступа

- Вредоносный запрос отправляется на веб-сервер FileWave MDM.
- Веб-сервер обрабатывает запрос, и из-за уязвимости ему не удаётся должным образом аутентифицировать запрос.
- Злоумышленнику предоставляется доступ super_user без необходимости использования действительных учётных данных пользователя.

4) Использование системы

- Имея доступ super_user, злоумышленник теперь может выполнять любые действия, которые мог бы выполнять легитимный администратор.
- Злоумышленник запрашивает у сервера MDM список всех управляемых устройств, извлекая конфиденциальную информацию, такую как серийные номера устройств, электронные письма пользователей, местоположения и т.д.
- Злоумышленник использует функциональные возможности MDM для отправки вредоносных пакетов или команд на управляемые устройства.

5) Выполнение вредоносных действий

- Злоумышленник устанавливает вредоносное программное обеспечение на управляемые устройства, такое как шпионское ПО или программы-вымогатели.
- В качестве альтернативы злоумышленник может изменить конфигурацию устройства, отключить параметры безопасности или выполнить другие вредоносные действия.