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. AirWatch MDM

Метод для обхода приложения intelligence HUB и прямой регистрации пользователей, эффективно обходя средства защиты MFA так как MFA применяется только в процессе первоначальной регистрации клиента MDM. Это означает, что после регистрации устройства последующие процессы аутентификации не требуют MFA, что делает их уязвимыми для атак с использованием однофакторной аутентификации (SFA).

A. Ключевые моменты реализации MFA

- **Первоначальная регистрация**: во время первоначальной регистрации устройства в AirWatch применяется MFA. Обычно это включает в себя ввод пользователем пароля и второй формы аутентификации, такой как одноразовый код-пароль (OTP), отправляемый на его мобильное устройство или электронную почту. Этот шаг гарантирует регистрацию устройства в системе MDM, снижая риск добавления неавторизованных устройств.
- **Пострегистрационная уязвимость**: после регистрации устройства последующие процессы аутентификации возвращаются к SFA. Это означает, что пользователям необходимо предоставить только одну форму аутентификации, обычно пароль, для доступа к службам MDM. Отсутствие постоянного применения MFA создаёт значительный пробел в системе безопасности, поскольку позволяет злоумышленникам использовать систему, если им удаётся получить учётные данные пользователя.
- **SFA**: уязвимости, связанные с SFA в AirWatch, могут использоватьсяed как до, так и параллельно с процессом регистрации, потенциально ставя под угрозу учётные данные пользователя или регистрируя вредоносные устройства.

B. Процесс начальной регистрации

- **Применение MFA**: во время первоначальной регистрации устройства в AirWatch применяется MFA. Обычно это включает в себя ввод пользователем пароля и второй формы аутентификации, такой как одноразовый код-пароль (OTP), отправляемый на его мобильное устройство или электронную почту. Этот шаг гарантирует надёжную регистрацию устройства в системе MDM, снижая риск добавления неавторизованных устройств.
- **Безопасная регистрация**: Процесс первоначальной регистрации предназначен для проверки личности пользователя и устройства. Требуя нескольких форм аутентификации, AirWatch гарантирует, что только легитимные пользователи и устройства могут завершить процесс регистрации. Этот процесс включает отправку адреса электронной почты или конечной точки сервера, который запускает discovery-запрос для определения местоположения соответствующей конечной точки MDM и получения необходимых сведений о конфигурации.

C. Уязвимость после регистрации

- **Возврат к SFA**: после регистрации устройства последующие процессы аутентификации возвращаются к SFA. Это означает, что пользователям необходимо предоставить только одну форму аутентификации, обычно пароль, для доступа к службам MDM. Отсутствие постоянного применения MFA создаёт значительный пробел в системе безопасности, поскольку позволяет злоумышленникам использовать систему, если им удаётся получить учётные данные пользователя.
- **Конечные точки аутентификации**: Определённые конечные точки API уязвимы для атак SFA. Эти конечные точки допускают атаки с использованием паролей и ограниченный список допустимых учётных записей домена.
- **Ограничения CAPTCHA и MFA**: хотя принудительное использование CAPTCHA и MFA применяются в процессе регистрации пользователя,

эти меры защиты не распространяются на последующие попытки аутентификации. Любая из функций API в AirWatch зависит от SFA, и предварительная регистрация пользователя не требуется для создания «поверхности атаки SFA». Все уязвимые конечные точки API общедоступны для злоумышленника, не прошедшего проверку подлинности, что позволяет осуществлять атаки с использованием паролей.

D. Атаки SFA в AirWatch MDM

1) Ключевые аспекты атаки SFA

- **Использование discovery-процесса**: Клиент AirWatch MDM инициирует discovery-процесс для определения местоположения соответствующей конечной точки MDM. Это включает отправку запроса в discovery-службу, которая возвращает конечную точку аутентификации и groupId (код активации), связанный с запрошенным доменом. GroupId считается общедоступной информацией и не защищён, что облегчает злоумышленникам получение этой важной информации.

- **Уязвимость конечных точек API**: Несколько конечных точек API идентифицированы как уязвимые для атак SFA. Эти конечные точки допускают парольные атаки и ограниченный список допустимых учётных записей домена: /deviceservices/enrollment/airwatchenroll.aws/validatelogincredentials и /deviceservices/authenticationendpoint.aws.

- **User Enumeration**: Возможность получения списка пользователей зависит от интегратора аутентификации и конфигурации конечной точки, что в случае успеха позволяет идентифицировать действительные имена пользователей, что упростило бы поиск конкретных учётных записей.

- **Обход CAPTCHA и MFA:** Принудительное использование CAPTCHA и MFA применяются только в процессе регистрации пользователя. После завершения регистрации используется исключительно SFA, что делает систему уязвимой для атак методом грубой силы. Злоумышленники могут сбросить такие значения, как InternalIdentifier или Универсальный идентификатор устройства (UDID) и active SessionID (SID), чтобы обойти защиту от CAPTCHA и выполнить попытки аутентификации без защиты личных данных.

2) Подробные сценарии атак

- **Использование discovery-службы**: Злоумышленники могут использовать discovery-службу для получения конечной точки аутентификации и groupId, чтобы отправлять запросы на сервер MDM, потенциально минуя первоначальные проверки безопасности.

- **Манипулирование идентификатором сеанса (SID)**: Значение SID легко восстановить, выполнив стандартный процесс регистрации MDM. Отправка POST-запроса в /DeviceManagement/Enrollment/EmailDiscovery возвращает SID проверки, который может быть использован в запросе validate-UserCredentials. Это значение SID затем может быть передано как часть параметризованного запроса для проверки-UserCredentials, что позволяет злоумышленникам обойти определённые проверки безопасности.

- **Раскрытие идентификатора groupId**: Значение groupId имеет решающее значение для выполнения любых дальнейших атак на среду. Все интерфейсы аутентификации AirWatch требуют представления значения groupId; без этой информации было бы невозможно выполнить аутентификационную атаку на среду. После восстановления значений endpoint и groupId AirWatch раскрывает параметры конфигурации среды MDM. Это также позволяет злоумышленнику, не прошедшему проверку подлинности, идентифицировать подгруппы, интеграции аутентификации и многочисленные дополнительные параметры конфигурации среды.

- **Уязвимость приложения boxer**: Приложение boxer поддерживает только SFA и не способно поддерживать MFA в его текущем виде. Это делает его постоянным интерфейсом SFA-атаки, который может быть использован для обхода всех средств защиты MFA, реализованных в наборе продуктов AirWatch. Обе функции Boxer registration и authentication API используют одну и ту же конечную точку API authenticationendpoint.aws. Переменным фактором в этом запросе является значение типа содержимого заголовка запроса. В процессе регистрации это значение заполняется как UTF-8, что позволяет отправлять текст сообщения в формате XML.

E. Функциональность AirWatch: Управление доступом в контейнерах

AirWatch предлагает надёжную платформу для управления мобильными устройствами в различных операционных системах и платформах. Функциональность управления контейнерным доступом AirWatch является краеугольным камнем её решения MDM, обеспечивающего безопасное, эффективное и гибкое управление мобильными устройствами в корпоративной среде. Предоставляя безопасное рабочее пространство, поддерживая управление BYOD и интегрируясь с корпоративными системами, AirWatch гарантирует, что организации смогут использовать преимущества мобильности без ущерба для безопасности.

- **Безопасное рабочее пространство**: AirWatch Container обеспечивает безопасное рабочее пространство на персональных устройствах, стирая чёткую границу между корпоративными и личными данными. Такое разделение гарантирует безопасное управление корпоративными ресурсами и доступ к ним без вторжения в личное пространство пользователя.

- **Управление BYOD**: Решение особенно полезно для управления собственным устройством (BYOD). Это позволяет компаниям распространять приложения Workspace ONE UEM и внутренние приложения в контейнере AirWatch, позволяя сотрудникам использовать свои мобильные устройства для работы без ущерба для безопасности.
- **Безопасность на уровне приложений**: AirWatch использует стандартную платформу набора для разработки программного обеспечения (SDK) для защиты корпоративных приложений в контейнере. Эта платформа гарантирует, что приложения видны внутри и снаружи контейнера AirWatch, но поддерживает строгие меры безопасности для корпоративных приложений с помощью кодов доступа к контейнеру и шифрования.
- **Аутентификация при едином входе**: Платформа поддерживает непрерывную аутентификацию при едином входе, позволяя пользователям безопасно получать доступ к корпоративным ресурсам через VPN-туннель приложений. Эта функция упрощает процесс входа в систему для пользователей, обеспечивая при этом безопасное управление доступом.
- **Связь с глобальной инфраструктурой**: функциональность AirWatch расширяется за счёт локализованного или облачного устройства, которое взаимодействует с глобальной инфраструктурой, поддерживаемой AirWatch, через домен awmdm.com. Такой глобальный охват гарантирует, что мобильные пользователи могут устанавливать безопасную связь с корпоративной средой независимо от своего местоположения.
- **Гибкое развёртывание**: AirWatch поддерживает гибридную модель развёртывания устройств, добавляя функциональность текущему развёртыванию и позволяя устройствам перенять настройки нужной организационной группы. Такая гибкость имеет решающее значение для организаций с различными политиками использования устройств, включая корпоративные модели, модели, принадлежащие сотрудникам, и модели бизнес-направлений.
- **Безопасность и шифрование**: Платформа стандартизирует стратегии обеспечения безопасности и предотвращения потери данных на мобильных устройствах. Он применяет код доступа / шифрование внутри контейнера AirWatch, предотвращая утечку данных за пределы приложения. Для устройств iOS он защищает данные с помощью шифрования FIPS 140-2 и поддерживает методы биометрической аутентификации, такие как Touch ID или EyeVerify.
- **Интеграция с корпоративными системами**: AirWatch легко интегрируется с существующими корпоративными системами, максимально увеличивая текущие инвестиции и расширяя эти возможности для управления мобильными устройствами. Эта интеграция жизненно важна для поддержания согласованного уровня безопасности во всех корпоративных ИТ-активах.
- **Комплексное управление электронной почтой и контентом**: AirWatch предлагает комплексные решения для мобильной электронной почты и управления контентом, гарантирующие безопасность корпоративной инфраструктуры электронной почты и сохранность конфиденциального контента в корпоративном контейнере. Эти функциональные возможности имеют решающее значение для поддержания целостности корпоративных данных на мобильных устройствах

F. Discovery-Процесс в AirWatch MDM

Discovery-процесс в решении AirWatch MDM является важным начальным этапом, который позволяет клиенту MDM найти соответствующую конечную точку аутентификации и получить необходимые сведения о конфигурации. Этот процесс необходим для надлежащего функционирования MDM-системы, гарантируя, что устройства могут безопасно подключаться к корпоративной сети.

1) Этапы discovery-процесса

- **Инициализация клиента**: когда пользователь запускает клиент AirWatch MDM на своём устройстве, ему предлагается ввести либо адрес электронной почты, либо конечную точку сервера. Эти входные данные используются для инициирования discovery-процесса.
- **Отправка discovery-запроса**: Клиент создаёт HTTP-запрос GET к discovery-службе AirWatch. Этот запрос отправляется на заранее определённый URL-адрес, обычно discovery.awmdm.com, и включает домен, связанный с адресом электронной почты пользователя.

```
http
GET
/autodiscovery/DeviceRegistry.aws/v2/d
omainlookup/domain/vmware.com
HTTP/1.1
Host: discovery.awmdm.com
User-Agent:
Agent/20.08.0.23/Android/11
Accept-Encoding: gzip, deflate
Connection: close
```

- **Заголовок авторизации**: Запрос включает заголовок авторизации и дополнительные проверки достоверности. Однако ни одна из этих сведений не проверяется на стороне сервера, что означает, что заголовок запроса можно значительно упростить без потери функциональности.

```
http
GET
/autodiscovery/awcredentials.aws/v2/domainlookup/domain/vmware.com
HTTP/1.1
Host: discovery.awmdm.com
User-Agent:
Agent/20.08.0.23/Android/11
Accept-Encoding: gzip, deflate
Connection: close
```

- **Ответ сервера**: Discovery-служба обрабатывает запрос и отвечает полезной нагрузкой JSON, которая включает конечную точку аутентификации и groupId (код активации), связанный с запрошенным доменом.

```
json
{
  "authenticationEndpoint":
"https://auth.awmdm.com",
  "groupID": "VMWprod"
}
```

- **groupId (код активации)**: groupId является обязательным значением для аутентификации в решении AirWatch. Он используется для связи регистрации общедоступного устройства с организацией заказчика. Несмотря на его важность, VMware не считает groupId конфиденциальной информацией, поскольку она общедоступна и не защищена.

2) Последствия для безопасности

- **Общедоступность**: Идентификатор группы и конечная точка аутентификации считаются общедоступной информацией. Это означает, что любой, кто знаком с доменом, может получить эти значения, которые потенциально могут быть использованы в дальнейших атаках на среду MDM.
- **Потенциал для использования**: Злоумышленники могут использовать discovery-службу для получения идентификатора groupId и конечной точки аутентификации. Располагая этой информацией, они могут отправлять запросы на сервер MDM, потенциально минуя первоначальные проверки безопасности и получая несанкционированный доступ.
- **Конечные точки API**: Существует несколько конечных точек API, которые участвуют в discovery-процессе:
  - /autodiscovery/awcredentials.aws/v1/domainlookup/domain/
  - /autodiscovery/awcredentials.aws/v2/domainlookup/domain/
  - /DeviceManagement/Enrollment/validate-userCredentials

Эти конечные точки возвращают важную информацию, которая может быть использована для дальнейшего использования MDM-системы.

- **Манипулирование идентификатором сеанса (SID)**: Значение SID легко восстановить, выполнив стандартный процесс регистрации MDM. Отправка POST-запроса в /DeviceManagement/Enrollment/EmailDiscovery возвращает SID проверки, который может использоваться в последующих запросах для проверки учётных данных пользователя.

G. Использование discovery-службы в AirWatch MDM

Discovery-служба в решении AirWatch MDM является важнейшим компонентом, который позволяет клиенту MDM находить соответствующую конечную точку аутентификации и получать необходимые сведения о конфигурации, такие как groupId. Однако этот сервис может быть использован злоумышленниками для получения информации, необходимой для дальнейших атак на окружение.

1) Как работает discovery-служба

- **Инициализация клиента**: когда пользователь запускает клиент AirWatch MDM на своём устройстве, ему предлагается ввести либо адрес электронной почты, либо конечную точку сервера. Эти входные данные используются для инициирования discovery-процесса.
- **Отправка discovery-запроса**: Клиент создаёт HTTP-запрос GET к discovery-службе AirWatch. Этот запрос отправляется на заранее определённый URL-адрес, обычно discovery.awmdm.com, и включает домен, связанный с адресом электронной почты пользователя.

```
http
GET
/autodiscovery/DeviceRegistry.aws/v2/domainlookup/domain/vmware.com
HTTP/1.1
Host: discovery.awmdm.com
User-Agent:
Agent/20.08.0.23/Android/11
Accept-Encoding: gzip, deflate
Connection: close
```

- **Ответ сервера**: Discovery-Служба обрабатывает запрос и отвечает полезной нагрузкой JSON, которая включает конечную точку аутентификации и groupId (код активации), связанный с запрошенным доменом.

```
json
{
  "authenticationEndpoint":
"https://auth.awmdm.com",
  "groupID": "VMWprod"
}
```

2) Использование discovery-службы

- **Общедоступность**: Идентификатор группы и конечная точка аутентификации считаются общедоступной информацией. Это означает, что любой, кто знаком с доменом, может получить эти значения, которые потенциально могут быть использованы в дальнейших атаках на среду MDM.
- **Упрощённые запросы**: Заголовок запроса можно значительно упростить без потери функциональности, поскольку ни одна информация не проверяется на стороне сервера. Это упрощает злоумышленникам обработку запросов к discovery-службе.

```
GET
/autodiscovery/awcredentials.aws/v2/do
mainlookup/domain/vmware.com
HTTP/1.1
Host: discovery.awmdm.com
User-Agent:
Agent/20.08.0.23/Android/11
Accept-Encoding: gzip, deflate
Connection: close
```

- **API Endpoints**:
  - /autodiscovery/awcredentials.aws/v1/domainlookup/domain/
  - /autodiscovery/awcredentials.aws/v2/domainlookup/domain/
  - /DeviceManagement/Enrollment/validate-userCredentials

Эти конечные точки возвращают важную информацию, которая может быть использована для дальнейшего использования MDM-системы.

- **Манипулирование идентификатором сеанса (SID)**: Значение SID легко восстановить, выполнив стандартный процесс регистрации MDM. Отправка POST-запроса в /DeviceManagement/Enrollment/EmailDiscovery возвращает SID проверки, который может использоваться в последующих запросах для проверки учётных данных пользователя.

3) Последствия использования discovery-службы

Используя discovery-службу, злоумышленники могут получить groupId и конечную точку аутентификации, которые необходимы для выполнения дальнейших атак на среду MDM. Эта информация позволяет злоумышленникам создавать запросы, которые могут обойти первоначальные проверки безопасности.

- **Раскрытие конфигурации**: После восстановления значений endpoint и groupId AirWatch раскрывает параметры конфигурации среды MDM. Это также позволяет злоумышленнику, не прошедшему проверку подлинности, идентифицировать подгруппы, интеграции аутентификации и многочисленные дополнительные параметры конфигурации среды.
- **User Enumeration**: Возможность получения списка пользователей зависит от интегратора аутентификации и конфигурации конечной точки и в случае успеха позволит идентифицировать действительные имена пользователей, что упростит поиск конкретных учётных записей.
- **Потенциал для дальнейших атак**: С помощью groupId и конечной точки аутентификации злоумышленники могут выполнять атаки с однофакторной аутентификацией (SFA), потенциально компрометируя учётные данные пользователя или регистрируя вредоносные устройства. Это может привести к несанкционированному доступу к корпоративным ресурсам и конфиденциальным данным.

H. Раскрытие конфигурации в AirWatch MDM

Используя discovery-службу для восстановления значений endpoint и groupId, злоумышленники могут раскрыть подробные параметры конфигурации среды MDM. В этом разделе даётся подробное объяснение того, как работает эта эксплуатация и её последствий.

1) Как работает раскрытие конфигурации

- **Использование discovery-службы**: Злоумышленники могут использовать discovery-службу для получения конечной точки аутентификации и groupId. Эти значения необходимы для выполнения дальнейших атак на среду MDM. Идентификатор группы, или код активации, является обязательным значением при попытке аутентификации в решении AirWatch. Хотя VMware не считает эту информацию конфиденциальной, она имеет решающее значение для дальнейшего использования.
- **Конечные точки API**: В discovery-процессе задействовано несколько конечных точек API, которые могут быть использованы для получения сведений о конфигурации:
  - /autodiscovery/awcredentials.aws/v1/domainlookup/domain/
  - /autodiscovery/awcredentials.aws/v2/domainlookup/domain/
  - /DeviceManagement/Enrollment/validate-userCredentials

Эти конечные точки возвращают важную информацию, которая может быть использована для дальнейшего использования MDM-системы.

- **Манипулирование идентификатором сеанса (SID)**: Значение SID легко восстановить, выполнив стандартный процесс регистрации MDM. Отправка POST-запроса в /DeviceManagement/Enrollment/EmailDiscovery возвращает SID проверки, который может

использоваться в последующих запросах для проверки учётных данных пользователя.

- **Раскрытие идентификатора groupId**: После восстановления значений конечной точки и groupId злоумышленники могут использовать конечную точку /deviceservices/enrollment/airwatchenroll.aws/validategroupidentifier для раскрытия параметров конфигурации среды MDM.

```
http
POST /deviceservices/enrollment/airwatchenroll.aws/validategroupidentifier HTTP/1.1
Host: vmware.awmdm.com
User-Agent: Agent/20.08.0.23/Android/11
Content-Length: 118
Content-Type: application/json
Accept-Encoding: gzip, deflate
Connection: close

{"Header":{"SessionId":"00000000-0000-0000-0000-000000000000"},"Device":{"InternalIdentifier":""},"GroupId":"VMWprod"}
```

2) *Последствия раскрытия конфигурации*

- **Подробная информация о конфигурации**: Ответ от конечной точки validategroupidentifier содержит подробные параметры конфигурации среды MDM. Эта информация может быть использована злоумышленниками для понимания структуры и конфигурации MDM-системы.

```
json
{
  "Header": {
    "ProtocolRevision": 0,
    "Language": null,
    "SessionId": "6debe689-709d-4f6a-b038-fe5f61fde336",
    "Mode": 2,
    "AgentToken": "978969b0-d2cf-4dd6-8e3c-eef546010b34",
    "ProtocolType": 0,
    "App": 0,
    "AppVersion": null
  },
  "Status": {
    "Code": 1,
    "Notification": ""
  },
  "NextStep": {
    "InstallUrl": "",
    "ServiceUrl": "https://vmware.awmdm.com/DeviceManagement/Enrollment/begin-samlAuthentication?sid=6debe689-709d-4f6a-b038-fe5f61fde336",
    "DeviceUserMode": 0,
    "StagingRequired": false,
    "DisplayStagingMessage": null,
    "UserIdentifier": null,
    "AfwProvisioningMode": 0,
    "RegistrationTypePo": 0,
    "RegistrationTypeDo": 0,
    "VidmForCico": false,
    "IsLbusEnabled": false,
    "ClosedNetworkEnrollment": false,
    "Type": 18,
    "SettingsPayload": "",
    "AgentSettings": null,
    "RequireServicesFromStore": false,
    "IsCaptchaRequired": false,
    "CaptchaValue": null,
    "AndroidEnrollmentTarget": 0,
    "KnoxPlayForWorkCapable": false,
    "AndroidWorkTempPassword": null,
    "UserEmailAddress": null,
    "showEnrollmentInfoMessages": false,
    "AFWUserAuthToken": null,
    "AFWAccountIdentifer": null,
    "IsDeviceAfwCertified": false,
    "GreenBoxUrl": null,
    "VidmServerUrl": null,
    "IsVidmConfigured": false,
    "IsGreenBoxCatalogEnabled": false,
    "IsContainerModeEnabled": false,
    "ScepPayload": null,
    "BeaconConsoleSettingsServer": null,
    "CollectImeiNumber": false,
    "IsCustomOnboardingExperienceEnabled": false,
    "CustomOnboardingMessage": null,
    "CustomOnboardingUserName": null,
    "CustomOnboardingWelcomeText": null
  }
}
```

- **Идентификация подгрупп**: Раскрытые параметры конфигурации включают информацию о подгруппах в среде MDM. Это позволяет злоумышленникам идентифицировать различные организационные подразделения и связанные с ними настройки.
- **Интеграция аутентификации**: В ответе также раскрываются подробности об интеграции аутентификации, например, настроена ли среда с использованием служб идентификации AirWatch, сторонних средств аутентификации или аутентификации на основе SAML.
- Значение типа в ответе указывает конфигурацию аутентификации:
  - **Тип 1**: Срок действия лицензии на оценку среды истёк или она не активна.
  - **Тип 2**: Среда настроена с использованием служб идентификации AirWatch и поддерживает SFA.

- **Тип 4**: Среда не настроена с помощью стороннего средства аутентификации и поддерживает SFA.
- **Тип 8**: Среда требует регистрации токена перед аутентификацией пользователя.
- **Тип 18**: Среда имеет интеграцию с SAML и требует MFA.

- **URL-адреса служб**: Ответ включает URL-адреса служб для проверки личности с помощью интеграций сторонних средств аутентификации. Эти URL-адреса могут быть использованы злоумышленниками для попытки аутентификации в контексте интегратора.
- **Потенциал для дальнейших атак**: с помощью раскрытой информации о конфигурации злоумышленники могут проводить более целенаправленные атаки на среду MDM. Это включает в себя выполнение атак с однофакторной аутентификацией (SFA), регистрацию вредоносных устройств и потенциальную компрометацию учётных данных пользователя.

I. Уязвимость конечных точек API в AirWatch MDM

Несколько конкретных конечных точек API в пакете продуктов VMware AirWatch для управления мобильными устройствами (MDM) уязвимы для атак с использованием однофакторной аутентификации (SFA), которые позволяют злоумышленникам выполнять атаки с использованием паролей и ограничивать количество действительных учётных записей домена.

1) Уязвимые Конечные точки API

- **Конечные точки discovery-службы:** /autodiscovery/awcredentials.aws/v1/domainlookup/domain/ ,/autodiscovery/awcredentials.aws/v2/domainlookup/domain/. Эти конечные точки используются в discovery-процессе для определения местоположения соответствующей конечной точки аутентификации MDM и получения groupId (кода активации). Ответы от этих конечных точек включают критическую информацию, такую как конечная точка аутентификации и groupId, которые необходимы для дальнейших атак.
- **Конечная точка проверки учётных данных пользователя:** /DeviceManagement/Enrollment/validate-UserCredentials. Для связи с этой конечной точкой требуется идентификатор сеанса (SID). SID можно легко восстановить, выполнив стандартный процесс регистрации MDM. Отправка POST-запроса в /DeviceManagement/Enrollment/EmailDiscovery возвращает SID проверки, который может быть использован в запросе validate-UserCredentials.
- **Конечная точка проверки учётных данных для входа:** /deviceservices/регистрация/airwatchenroll.aws/validatelogincredentials. Эта конечная точка используется приложением Intelligence HUB в процессе регистрации пользователя для проверки учётных данных пользователя. Даже если в среде настроена аутентификация сторонних производителей, этот API по-прежнему предоставляется в качестве интерфейса связи.
- **Конечная точка аутентификации**: /deviceservices/authenticationendpoint.aws. Эта конечная точка используется в двух функциях почтового агента Boxer: регистрации и аутентификации. Приложение Boxer поддерживает только SFA и не способно поддерживать MFA в его текущем виде, что делает его постоянным интерфейсом атаки SFA.

2) Эксплуатация уязвимых конечных точек API

- **Использование discovery-службы**: злоумышленники могут использовать конечные точки discovery-службы для получения конечной точки аутентификации и groupId. Располагая этой информацией, они могут отправлять запросы на сервер MDM, потенциально минуя первоначальные проверки безопасности и получая несанкционированный доступ.
- **Манипулирование идентификатором сеанса (SID)**: Значение SID легко восстановить, выполнив стандартный процесс регистрации MDM. Отправка POST-запроса в /DeviceManagement/Enrollment/EmailDiscovery возвращает SID проверки, который может использоваться в последующих запросах для проверки учётных данных пользователя.
- **User enumeration**: Возможность получения списка пользователей зависит от интегратора аутентификации и конфигурации конечной точки и позволяет бы злоумышленникам идентифицировать действительные имена пользователей, что упростило бы поиск конкретных учётных записей.
- **Парольные атаки**: уязвимые конечные точки API допускают парольные атаки, при которых злоумышленники могут систематически пробовать различные комбинации паролей для получения доступа. Отсутствие постоянного применения MFA облегчает злоумышленникам успех этих атак.

3) Примеры запросов и ответов API

Discovery-запрос:

```
http
GET
/autodiscovery/awcredentials.aws/v2/domainlookup/domain/vmware.com
HTTP/1.1
Host: discovery.awmdm.com
User-Agent:
Agent/20.08.0.23/Android/11
Accept-Encoding: gzip, deflate
Connection: close
```

Discovery Response:
Example of a discovery response:
json
{
"authenticationEndpoint": "https://auth.awmdm.com",
"groupID": "VMWprod"
}

Validate User Credentials Request:
Example of a validate-userCredentials request:
http
GET /DeviceManagement/Enrollment/validate-userCredentials?groupid=True&welcome=False&id=1e69ee15-4749-44fe-8d91-a67bf7fd971e HTTP/1.1
Host: vmware.awmdm.com
User-Agent: Agent/20.08.0.23/Android/11
Content-Length: 0
Accept: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: close

Validate Login Credentials Request:
Example of a validatelogincredentials request:
json
{
"Username": "test",
"Password": "test",
"Header": {
"SessionId": "f4e74df0-f22f-48f5-9496-1d5b66526ed3"
},
"SamlCompleteUrl": "aw://",
"Device": {
"InternalIdentifier": "3c411751c74c4f6cbceac8e39dd053d4c226d78d"
}
}

Authentication Endpoint Request:
Example of a Boxer authentication request:
json
{
"ActivationCode": "aCode",
"BundleId": "com.box.email",
"Udid": "409853f111044398a463119d878f34665e23271f",
"Username": "test",
"AuthenticationType": "2",
"RequestingApp": "com.boxer.email",
"DeviceType": "2",
"Password": "test",
"AuthenticationGroup": "com.air-watch.boxer"
}

}

J. Смягчение последствий "Integrating SAML/IDP/MFA "

Хотя интеграция служб SAML / IdP / MFA в процессе регистрации пользователя в AirWatch MDM повышает безопасность, ограничения приложения boxer и отсутствие постоянного обеспечения соблюдения MFA создают значительные уязвимости. Внедрение постоянного применения MFA и дополнительных мер безопасности может помочь снизить эти риски и защитить среду MDM от потенциальных атак.

1) Интеграция SAML/ IDP/ MFA

- **Цель SAML/IDP/MFA**: Интеграция служб SAML, поставщика идентификационных данных (IdP) и многофакторной аутентификации (MFA) направлена на повышение безопасности процесса аутентификации. Эти сервисы предоставляют дополнительные уровни проверки, затрудняя получение несанкционированного доступа.

- **Процесс регистрации пользователя**: VMware предполагает, что интеграция SAML / IdP / MFA в первую очередь поддерживается в процессе регистрации пользователя через приложение intelligence HUB. Это означает, что при регистрации нового устройства или пользователя может быть применён MFA для обеспечения безопасности регистрации. Приложение Intelligence HUB взаимодействует с сервером AirWatch MDM для проверки учётных данных пользователя и применения MFA на этом начальном этапе регистрации.

- **Этапы настройки**: Для реализации служб SAML / IdP администраторам необходимо настроить workspace ONE Access (ранее VMware identity Manager) на выполнение функций поставщика удостоверений. Это включает в себя настройку метаданных SAML, настройку параметров поставщика удостоверений и включение аутентификации SAML как для консоли администратора, так и для портала самообслуживания.
  - Загрузка метаданных поставщика удостоверений (IdP) из Workspace ONE Access.
  - Загрузка метаданных IdP в консоль AirWatch в разделе Настройки служб каталогов.
  - Включение аутентификации SAML для консоли администратора и портала самообслуживания.
  - Настройка политик доступа для обеспечения соблюдения MFA в процессе регистрации.

- **Интеграция с Workspace ONE Access**: Workspace ONE Access предоставляет единую платформу для управления идентификацией и доступом в различных службах VMware, включая AirWatch MDM. Он поддерживает интеграцию со сторонними

поставщиками идентификационных данных и решениями единого входа, такими как Okta, обеспечивая бесперебойную аутентификацию. Интеграция гарантирует, что пользователи смогут использовать существующие решения для управления идентификацией для аутентификации в среде AirWatch MDM.

2) Ограничения и проблемы

- **Ограничение приложения Boxer**: Одним из существенных ограничений является то, что приложение Boxer, входящее в состав пакета AirWatch MDM suite, поддерживает только однофакторную аутентификацию (SFA). Это означает, что даже если сервисы SAML / IdP / MFA реализованы в процессе регистрации, приложение Boxer не применяет MFA для последующих аутентификаций. Неспособность приложения Boxer поддерживать MFA создаёт постоянную уязвимость для получения несанкционированного доступа.

- **Уязвимость после регистрации**: в то время как MFA применяется во время процесса первоначальной регистрации, последующие процессы аутентификации возвращаются к SFA. Это означает, что после регистрации устройства пользователям необходимо предоставить только одну форму аутентификации, обычно пароль, для доступа к службам MDM. Отсутствие постоянного обеспечения соблюдения MFA делает систему уязвимой для компрометации учётных данных и несанкционированного доступа.

K. Устранение "Отключения Enrollment в Boxer"

Хотя отключение служб регистрации boxer предлагается в качестве потенциального шага по устранению уязвимостей, связанных с SFA-атаками в AirWatch MDM, его эффективность сомнительна. Разъяснения VMware и внедрение комплексных мер безопасности необходимы для эффективного сокращения поверхности атаки и повышения общей безопасности среды MDM.

1) Понимание Регистрации Boxer

Boxer — это почтовое клиентское приложение, входящее в состав пакета AirWatch MDM suite. Он предназначен для обеспечения безопасного доступа к электронной почте на мобильных устройствах, управляемых AirWatch. Приложение поддерживает однофакторную аутентификацию (SFA), но, по сути, не поддерживает многофакторную аутентификацию (MFA).

Службы регистрации Boxer отвечают за первоначальную настройку и регистрацию приложения Boxer на устройствах пользователей. Этот процесс включает проверку подлинности учётных данных пользователя и привязку устройства к учётной записи электронной почты пользователя в среде AirWatch.

2) Отключение служб регистрации Боксеров

- **Предлагаемые меры по устранению неполадок**: VMware предполагает, что отключение служб регистрации Boxer потенциально может уменьшить уязвимости, связанные с атаками SFA. Этот шаг предотвратит регистрацию новых устройств в приложении Boxer, что потенциально уменьшит поверхность атаки.

- **Неопределённость в отношении аутентификации Конечная точка API**: конечная точка API аутентификации имеет решающее значение для процесса регистрации и последующих аутентификаций. Если эта конечная точка остаётся активной, злоумышленники все равно могут использовать её для SFA-атак, даже если службы регистрации Boxer отключены.

- **Прочее**: Эффективность этого этапа смягчения зависит от степени, в которой он влияет на общую поверхность атаки. Если отключение служб регистрации Boxer не приведёт к удалению конечной точки API аутентификации, поверхность атаки может быть незначительно уменьшена. Злоумышленники потенциально могут найти альтернативные способы использования системы, используя конечную точку API активной аутентификации.

3) Выводы и рекомендации

- **Комплексные меры безопасности**: Организациям следует рассмотреть возможность внедрения комплексных мер безопасности, помимо отключения служб регистрации boxer. Это включает в себя применение многофакторной аутентификации (MFA) во всех точках доступа, регулярный аудит конфигураций безопасности и обучение пользователей передовым методам обеспечения безопасности.

- **Непрерывный мониторинг**: Необходим непрерывный мониторинг среды AirWatch и приложения Boxer. Организациям следует отслеживать необычную активность, которая может указывать на попытку эксплуатации, и оперативно реагировать на потенциальные инциденты безопасности.

- **Альтернативные решения**: Изучение альтернативных решений или конфигураций, которые по своей сути поддерживают MFA для доступа к электронной почте на мобильных устройствах, может обеспечить более надёжную защиту. Это может включать использование различных почтовых клиентов, которые полностью интегрируются с решениями MFA, или улучшение конфигураций безопасности в пакете AirWatch MDM suite.

L. Устранение "Отключение discovery-служб"

Отключение discovery-служб в AirWatch MDM - рекомендуемый шаг по смягчению последствий, позволяющий предотвратить публичное раскрытие конечной точки AirWatch и groupId. Однако эта мера имеет ограниченное значение для предотвращения атак, поскольку значение groupId может быть введено методом

перебора. Для эффективной защиты среды AirWatch MDM организациям необходимо внедрить комплексные меры безопасности, включая непрерывное применение MFA, регулярные аудиты безопасности и обучение пользователей. Эти шаги могут помочь снизить риски, связанные с общедоступностью критически важной информации, и повысить общую безопасность среды MDM.

1) *Понимание discovery-служб*

- **Функциональность discovery-службы**: Discovery-служба в AirWatch MDM отвечает за определение местоположения соответствующей конечной точки аутентификации MDM и получение groupId (кода активации). Этот процесс инициируется, когда пользователь указывает адрес электронной почты или конечную точку сервера во время начальной настройки клиента AirWatch MDM. Discovery-запрос отправляется на заранее определённый URL-адрес, обычно discovery.awmdm.com, и включает домен, связанный с адресом электронной почты пользователя. Ответ от discovery-службы включает конечную точку аутентификации и groupId.

- **Общедоступность**: Идентификатор группы и конечная точка аутентификации считаются общедоступной информацией. VMware не классифицирует эту информацию как конфиденциальную, что означает, что она доступна любому, кто разбирается в предметной области. Такая общедоступность является ключевым фактором потенциального использования discovery-службы.

2) *Отключение discovery-служб*

- **Предлагаемые меры по смягчению последствий**: Отключение discovery-служб предлагается в качестве меры по смягчению последствий, чтобы предотвратить публичное раскрытие конечной точки AirWatch и groupId. Отключая эти службы, организации стремятся снизить риск получения злоумышленниками важной информации, которая может быть использована в дальнейших атаках.

- **Реализация**: Отключение discovery-служб включает настройку среды AirWatch MDM для ограничения или исключения использования конечных точек discovery-службы. Это может быть достигнуто с помощью административных настроек или элементов управления сетевого уровня для блокирования доступа к URL-адресам discovery-службы.

3) *Ограничения отключения discovery-служб*

- **Принудительное использование groupId**: отключение discovery-служб имеет ограниченное значение для предотвращения атак, поскольку значение groupId может быть принудительно введено. Злоумышленники могут систематически пробовать разные значения groupId, пока не найдут правильное, минуя discovery-службу. groupId — это относительно короткое и предсказуемое значение, что позволяет злоумышленникам использовать автоматизированные инструменты для перебора допустимых значений groupId.

- **Важная информация для дальнейших атак**: несмотря на то, что groupId не считается конфиденциальным, он важен для проведения дальнейших атак на среду AirWatch. Все интерфейсы аутентификации AirWatch требуют представления значения groupId. Без этой информации было бы невозможно выполнить аутентификационную атаку на среду.

- **Общедоступные конечные точки API**: Многие конечные точки API в AirWatch MDM являются общедоступными и не требуют предварительной аутентификации. Это означает, что даже если discovery-службы отключены, злоумышленники все равно могут взаимодействовать с этими конечными точками, используя принудительно введённые значения groupId.

4) *Практические последствия*

- **Ограниченная эффективность**: одного отключения discovery-служб недостаточно для обеспечения безопасности среды AirWatch MDM. Хотя это может добавить слой неясности, это не решает фундаментальную проблему, связанную с возможностью принудительного использования groupId и общедоступностью критических конечных точек API.

- **Комплексные меры безопасности**: для эффективного снижения рисков организациям необходимо внедрить комплексные меры безопасности, которые выходят за рамки отключения discovery-служб. Это включает в себя применение многофакторной аутентификации (MFA) для всех процессов аутентификации, регулярный аудит конфигураций безопасности и мониторинг необычных действий.

- **Непрерывное применение MFA**: Обеспечение применения MFA не только в процессе первоначальной регистрации, но и при последующих аутентификациях может значительно повысить безопасность. Это затруднило бы злоумышленникам использование значений groupId с принудительным использованием.

- **Обучение пользователей**: Информирование пользователей о важности методов обеспечения безопасности, таких как отказ от предоставления своего идентификатора группы и осторожное отношение к попыткам фишинга, может помочь снизить риск эксплуатации.