Kaspersky ICS CERT

kaspersky

Секреты протокола Schneider Electric UMAS

Павел Нестеров
Никита Комаров
Андрей Муравитский

29.09.2022 Version 1.2

UMAS (Unified Messaging Application Services) — это проприетарный протокол Schneider Electric, который используется для конфигурации и мониторинга Schneider Electric PLC.

UMAS используют такие контроллеры Schneider Electric, как Modicon M580 CPU (part numbers BMEP* and BMEH*), Modicon M340 CPU (part numbers BMXP34*). Конфигурация и программирование осуществляется при помощи инженерного ПО — EcoStruxure™ Control Expert (Unity Pro), EcoStruxure™ Process Expert и т.п.

В 2020 году стало известно об уязвимости CVE-2020-28212, эксплуатация которой позволяет удаленному неавторизованному атакующему получить управление контроллером с правами уже аутентифицированного на ПЛК оператора. После выявления этой уязвимости компания Schneider Electric разработала новый механизм — Application Password, — который должен предоставлять защиту от несанкционированного доступа к ПЛК и внесения нежелательных изменений.

Анализ, проведенный специалистами Kaspersky ICS CERT, показал, что новый механизм защиты также реализован с недостатками. Выявленная в ходе исследования уязвимость CVE-2021-22779 позволяет удаленному нарушителю обойти процесс аутентификации при внесении изменений на ПЛК.

Удалось установить, что протокол UMAS в реализации до исправления уязвимости CVE-2021-22779 имеет существенные недостатки, которые критически влияют на безопасность систем управления на основе контроллеров Schneider Electric.

К середине августа 2022 года Schneider Electric выпустил обновление для программного обеспечения EcoStruxure™ Control Expert и ПЛК Modicon M340 с исправлением данной уязвимости. В марте 2023 года вендор выпустил обновление для ПЛК Modicon M580.

В отчёте описаны:

- реализация протокола UMAS без использования защитного механизма Application Password;
- обход аутентификации без использования Application Password;
- принцип работы защитного механизма Application Password;
- механизмы эксплуатации уязвимости CVE-2021-22779 (обход аутентификации с настроенным Application Password);
- принцип работы обновленного процесса резервирования устройства.

В заключении приведены меры для устранения уязвимости обхода аутентификации от Schneider Electric и рекомендации Kaspersky ICS CERT.

Если вам нужно больше информации или вы хотите поделиться своими мыслями по данной теме, напишите на адрес ics-cert@kaspersky.com.

Snort правила доступны на портале Kaspersky Threat Intelligence (ICS Reporting).

Объект исследования

UMAS (Unified Messaging Application Services) — проприетарный протокол Schneider Electric, который используется для конфигурации, мониторинга сбора данных и управления промышленными контроллерами Schneider Electric.

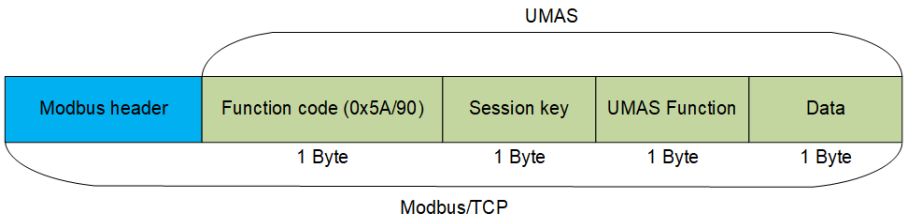
UMAS основан на клиент-серверной архитектуре. В ходе нашего исследования в качестве клиента было использовано программное обеспечение для конфигурации ПЛК EcoStruxure™ Control Expert, в качестве сервера — контроллер Modicon M340 CPU.

Протокол UMAS

Строение сетевого пакета

UMAS основан на протоколе Modbus/TCP.

Структурная схема протокола UMAS



В спецификации протокола Modbus/TCP определены зарезервированные значения Function Code, которые могут быть использованы разработчиками для своих нужд. С полным списком зарезервированных значений можно ознакомиться в официальной документации.

Schneider Electric использует Function Code 90 (0x5A) для определения того, что значение поля Data сформировано в соответствии протоколу UMAS.

Ниже показана структура сетевого пакета на примере запроса чтения блока памяти (pu_ReadMemoryBlock) ПЛК:

- Красный: Function code 90 (0x5A)
- Синий: Session key 0 (0x00) (см. Session key)
- Зелёный: UMAS функция 20 (0x20) (см. Функции)
- Оранжевый: Data

Каждая функция имеет определенный набор информации в Data. Например, смещение от базового адреса памяти, размер передаваемой информации, номер блока памяти и т.д.

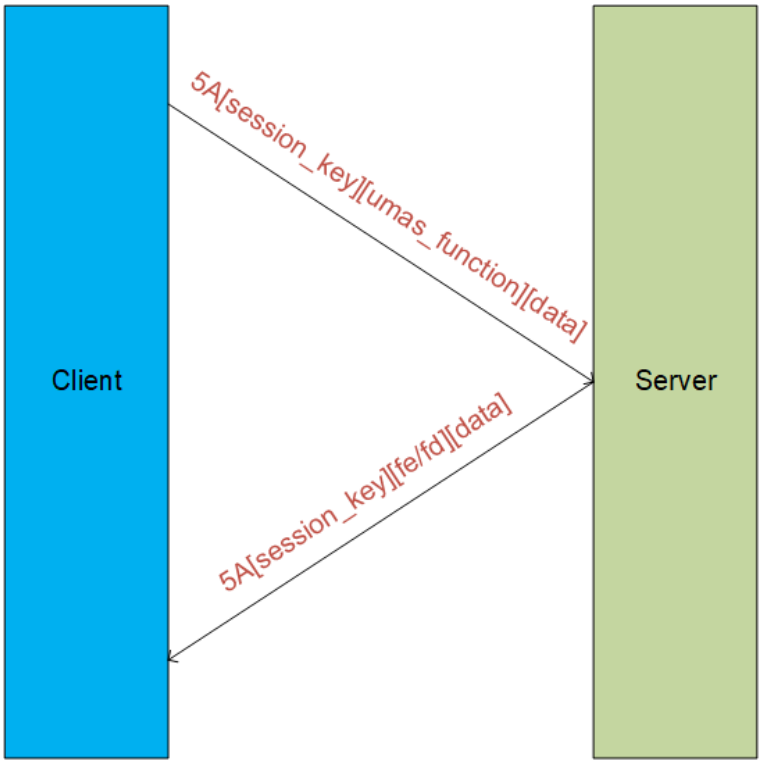
```
    112 2.233067    192.168.0.6     192.168.0.150   UMAS    73 [19] UMAS: ReadMemoryBlock
    114 2.245383    192.168.0.150   192.168.0.6     UMAS    579 [525] UMAS: Response
<
> Frame 112: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{F658B7F2-24EC
> Ethernet II, Src: VMware_d5:a0:80 (00:0c:29:d5:a0:80), Dst: Telemech_25:c6:36 (00:80:f4:25:c6:36)
> Internet Protocol Version 4, Src: 192.168.0.6, Dst: 192.168.0.150
> Transmission Control Protocol, Src Port: 57651, Dst Port: 502, Seq: 2423, Ack: 5209, Len: 19
v Schneider UMAS Protocol
    Transaction id: 57589
    Protocol id: 0
    Data length: 13
    Unit id: 0
    Function: 90
    Connection id: 0
    Command: 0x20
    Sys Ram block number: 276
    Sys Ram address: 0
    Size: 0
    Data: 000002

0000  00 80 f4 25 c6 36 00 0c  29 d5 a0 80 08 00 45 00
0010  00 3b d2 f6 40 00 80 06  a5 d9 c0 a8 00 06 c0 a8
0020  00 96 e1 33 01 f6 71 2d  36 68 b7 64 58 0c 50 18
0030  fd a8 b1 62 00 00 e0 f5  00 00 00 0d 00 5a 00 20
0040  01 14 00 00 00 00 00 00  02
```

Сетевое взаимодействие

UMAS наследует и клиент-серверную архитектуру Modbus. Ниже показана структурная схема взаимодействия клиента и сервера.

Схема взаимодействия клиента (EcoStruxure™ Control Expert) и сервера (ПЛК)



В сетевом пакете UMAS сразу после Function code 0x5A следует Session key — ключ текущей сессии.

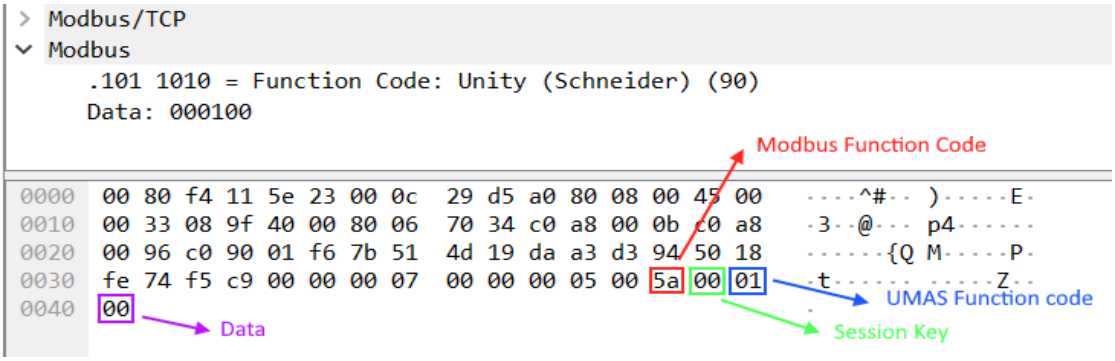
Блок-схема сетевого пакета UMAS

Рассмотрим взаимодействие между клиентом и сервером (ПЛК, далее также «устройство») на примере анализа фрагмента реального трафика.

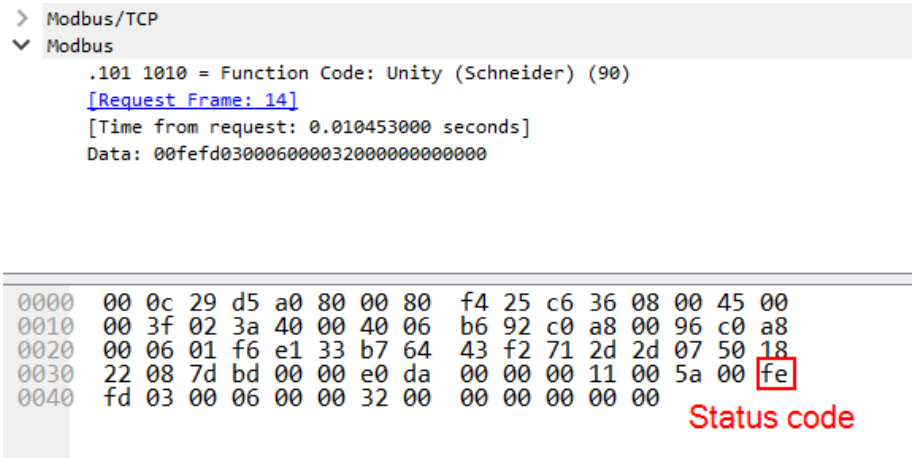
На скриншоте ниже показан пакет, отправленный клиентом (EcoStruxure™ Control Expert) серверу (PLC) с функцией **umas_QueryGetComInfo(0x01)**.

Структура данной функции:

```
TCP DATA — Modbus Header — 0x5A — session — 01(UMAS function code) — 00(data).
```



Устройство должно отправлять ответ на каждый отправленный запрос. На скриншоте ниже показан ответ устройства клиенту:



Status code — это статус выполнения устройством функции, которая была отправлена ему клиентом в предыдущем запросе. Значение «0xFE» обозначает успешное выполнение функции, «0xFD» — ошибку. Данные значения находятся в каждом ответе устройства на запрос с функцией от клиента. Status code всегда располагается сразу после session key.

Процедура резервирования

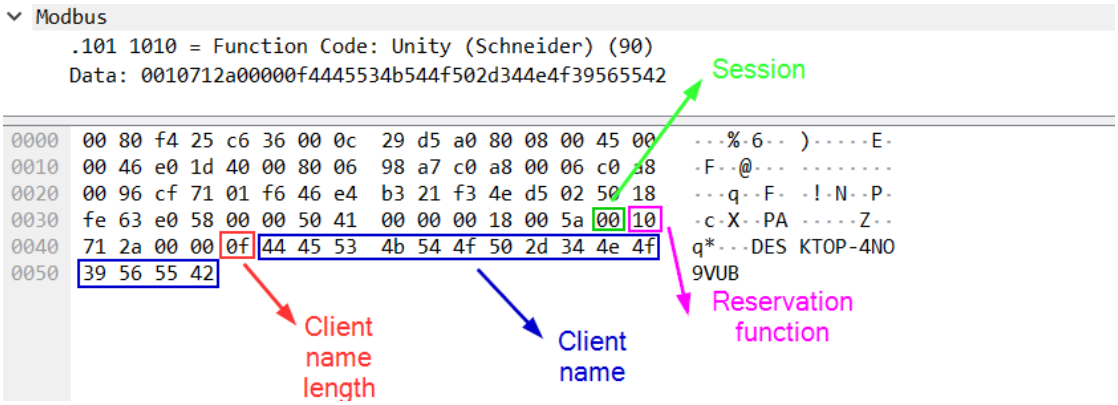
Для внесения изменений в ПЛК требуется его «резервирование». Данная процедура выполняет роль аутентификации.

Только один клиент (например, рабочая станция инженера) может зарезервировать устройство-сервер в один момент времени для его конфигурации или мониторинга состояния. Это необходимо для предотвращения внесения параллельных несогласованных изменений в устройство.

Ниже на скриншоте представлен запрос на выполнение процедуры резервирования устройства в базовом варианте (без использования защитного механизма Application Password).

Для резервирования устройства используется функция **umas_QueryTakePLCReservation(0x10).**

Клиент отправляет устройству запрос с функцией 0x10 для резервирования устройства. Данный запрос также содержит имя клиента, который резервирует устройство, и значение длины данного имени.



Session key

При завершении резервирования устройство передает клиенту значение нового однобайтового ключа сессии. Ключ используется далее для авторизации запросов на изменение устройства.

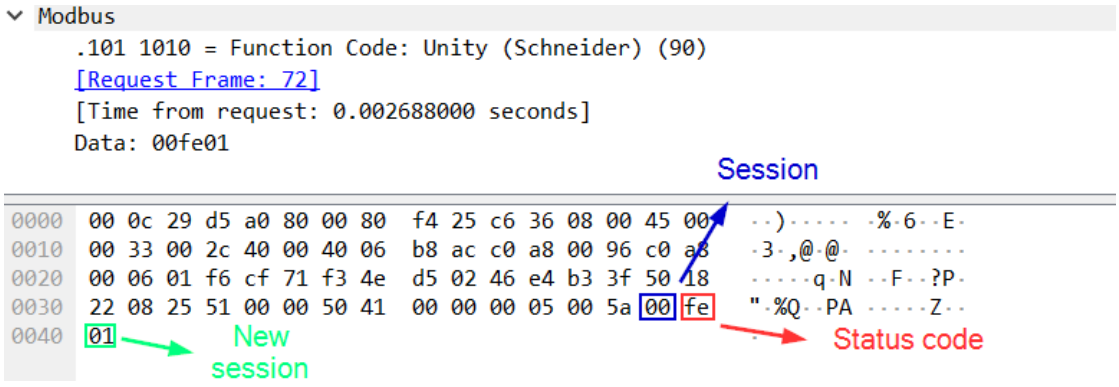
По мере выхода новых версий прошивок механизм создания сессии претерпел некоторые изменения, а именно:

1. До версии прошивки 2.7 для устройства Modicon M340 ключ сессии после резервирования устройства имел фиксированное значение 0x01;

2. После версии прошивки 2.7 для устройства Modicon M340 ключ сессии после резервирования устройства имел случайное значение, т.е. от 0 до 0xFF, так как длина ключа сессии — 1 байт.

До завершения резервирования используется сервисная сессия со значением «0x00». С её помощью можно выполнять функции, которые не требуют резервирования.

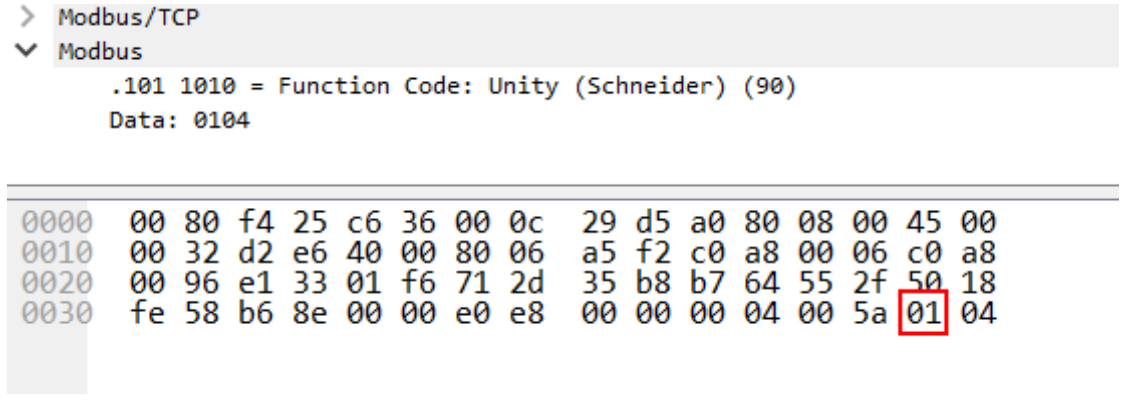
Ответ устройства, который содержит в себе Status code (0xfe) и новый session key, будет выглядеть так:



Status code «fe» означает что процедура резервирования прошла успешно.

В этом случае устройство передаст значение нового ключа сессии. Во всех последующих запросах в рамках текущей «зарезервированной» сессии используется новый ключ сессии.

На следующем скриншоте показан запрос от клиента к устройству сразу после успешного резервирования с использованием нового ключа сессии. В данном запросе используется функция **ex_GetPlcStatus(0x04).**



Поскольку процедура резервирования выполняет роль аутентификации для внесения изменений в устройства, данный механизм является критически важным с точки зрения безопасности.

О проблемах резервирования устройства с настройками по умолчанию и с защитными механизмами мы расскажем в следующих разделах.

Функции протокола UMAS

Протокол UMAS имеет множество функций для взаимодействия с целевым устройством. Функции можно разделить на 2 группы:

1. Функции, которые требуют резервирования устройства. Как правило, это функции для внесения изменений в ПЛК.
2. Функции, которые не требуют резервирования устройства. Такие функции не вносят изменения в ПЛК и не влияют на его работу.

Ниже представлен сокращенный список функций протокола UMAS. Необходимость резервирования устройства для представленных функций актуальна для версии прошивки 3.30 для устройства Modicon M340 без использования защитного механизма Application Password.

Функции, относящиеся к процессу резервирования устройства

1. 0x10 — umas_QueryTakePLCReservation — резервирование устройства.
2. 0x11 — umas_QueryReleasePLCReservation — освобождение устройства от резервирования.
3. 0x12 — umas_QueryKeepPLCReservation — статус резервирования.

Функции, которые требуют резервирования устройства

Функции инициализации

0x01 — umas_QueryGetComInfo — инициализация UMAS сообщения.

Функции для запроса информации об устройстве

1. 0x02 — pu_GetPlcInfo — запрос информации об устройстве
2. 0x04 — pu_GetPlcStatus — запрос статуса ПЛК
3. 0x06 — pu_GetMemoryCardInfo — запрос информации о SD карте устройства

Функции для загрузки и выгрузки стратегии ПЛК

Стратегия — это набор инструкций и данных, используемых ПЛК для выполнения его главной функции — управления конечным оборудованием, например, для автоматизации определенного технологического процесса.

1. 0x30 — pumem_BeginDownload — инициализация загрузки с ПК на ПЛК.
2. 0x31 — pumem_DownloadPacket — загрузка блока стратегии с ПК на ПЛК.
3. 0x32 — pumem_EndDownload — завершение процесса загрузки с ПК на ПЛК.

4. 0x33 — pumem_BeginUpload — инициализация выгрузки с ПЛК на ПК.
5. 0x34 — pumem_UploadPacket — выгрузка блока стратегии с ПЛК на ПК.
6. 0x35 — pumem_EndUpload — завершения процесса выгрузки с ПЛК на ПК.

Функции, которые не требуют резервирования устройства

Функции чтения значений из памяти устройства

0x20 — pu_ReadMemoryBlock — чтение блока памяти ПЛК.

Функция записи значений в память устройства

0x21 — pu_WriteMemoryBlock — запись блока памяти ПЛК.

Функции управления состоянием ПЛК

С помощью следующих функций можно запустить или приостановить работу ПЛК. Данные функции не требуют резервирования, если не активирован защитный механизм Application Password, тогда устройство успешно обработает запрос с использованием сервисной сессии (0x00) (см. Session key).

Если Application Password не используется, атакующий с помощью данных функций может остановить работу ПЛК и тем самым нанести существенный вред технологическому процессу.

1. 0x40 — ex_StartTask — запуск работы ПЛК.
2. 0x41 — ex_StopTask — остановка работы ПЛК.

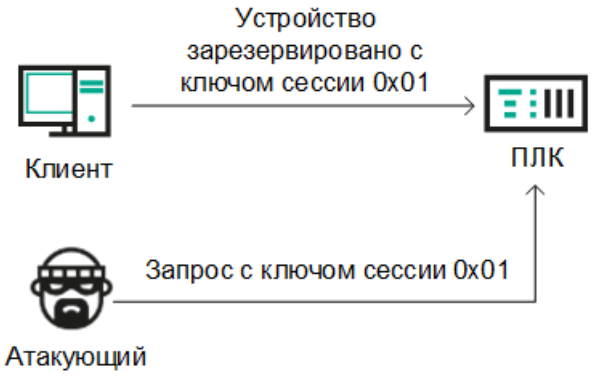
CVE-2020-28212: обход аутентификации без использования механизма Application Password

Основная проблема базового механизма резервирования, без использования Application Password, в том, что атакующий с помощью ключа сессии может отправлять запросы и изменять конфигурацию устройства.

До версии прошивки 2.7 для устройства Modicon M340 ключ сессии после каждого резервирования устройства имеет одно и то же значение и равен «0x01». Соответственно, атакующий может вносить изменения на устройстве вызывая соответствующие функции, предварительно зарезервировав устройство самостоятельно, или после того, как устройство было зарезервировано легитимным пользователем.

Схема атаки выглядит следующем образом:

Схема атаки удаленного злоумышленника. Версия прошивки ПЛК Modicon M340 до 2.7, устройство зарезервировано инженером



Если в момент атаки устройство не зарезервировано, атакующий с помощью функции **umas_QueryTakePLCReservation(0x10)** может сам зарезервировать устройство для последующих изменений.

После версии прошивки 2.7 для устройства Modicon M340 ключ сессии после резервирования устройства принимает случайное значение. Однако длина идентификатора сессии составляет всего один байт, соответственно, максимально возможное количество значений идентификатора сессии равно 256. Это позволяет удаленному неавторизованному нарушителю произвести подбор уже установленного идентификатора сессии между легитимным пользователем и ПЛК методом перебора.

Для выполнения такого типа атаки удаленному нарушителю, необходимо отправить ряд сетевых запросов на порт 502/TCP ПЛК с разными идентификаторами сессии и посмотреть на возвращаемый ответ от ПЛК. В случае если идентификатор сессии был подобран правильно, нарушитель получит статус код `0xfe`, означающий успешное выполнение запроса. В противном случае нарушитель получит статус код `0xfd`.

Описанные выше действия можно имплементировать с помощью любого языка программирования, атакующему не обязательно использовать EcoStruxure™e Control Expert или другое специализированное ПО для взаимодействия с устройством.

Application Password

С целью нивелирования ранее выявленной уязвимости CVE-2020-28212, эксплуатация которой позволяла удаленному неавторизованному атакующему получить возможность управления ПЛК с правами уже аутентифицированного на ПЛК оператора, компания Schneider Electric разработала новый механизм защиты. По замыслу Schneider Electric, имплементация улучшенного механизма защиты, основанного на использовании криптографических алгоритмов вычисления идентификатора

сессии и увеличении его длины, должна была предотвратить возможность подбора однобайтовой сессии.

С версии прошивки 3.01 для устройства Modicon M340 Schneider Electric начала активно развивать механизмы безопасности для предотвращения использования злоумышленником UMAS функций для внесения изменений в работу устройства. Для реализации аутентификации между клиентом и устройством необходимо установить Application Password в настройках проекта («Project & Controller Protection»). По своей сути данный механизм должен предоставлять защиту от несанкционированного доступа, нежелательных изменений, загрузки и выгрузки стратегии ПЛК.

После активации данного механизма с помощью EcoStruxure™ Control Expert клиенту необходимо вводить пароль при подключении к устройству в рамках процедуры резервирования.

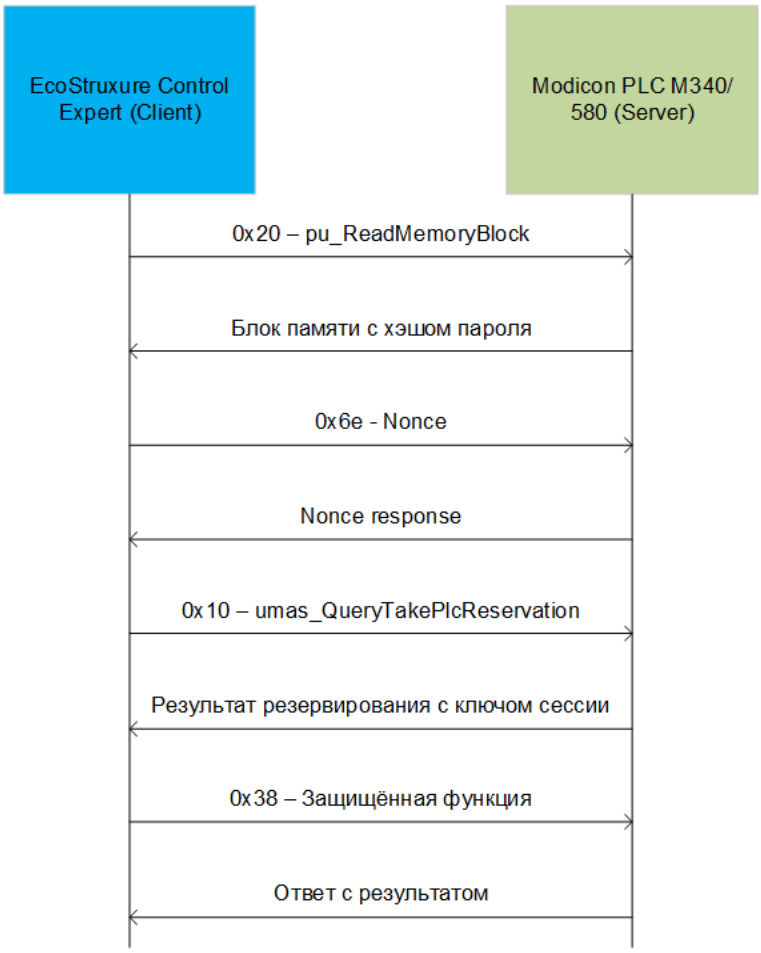
Также Application Password вносит изменения в сам механизм резервирования. Эти изменения будут рассмотрены в следующих разделах.

Обход аутентификации с использованием механизма Application Password

Анализ, проведенный специалистами Kaspersky ICS CERT, показал, что новый механизм защиты, к сожалению, также оказался реализован с недостатками. Выявленная в ходе исследования уязвимость CVE-2021-22779 позволяет удаленному нарушителю обойти процесс аутентификации и использовать функции, требующие резервирования, чтобы вносить изменения в ПЛК.

Для более полного понимания того, в чем заключаются недостатки «улучшенного» механизма защиты, рассмотрим процесс аутентификации и резервирования ПЛК более подробно. Новый механизм защиты основан на обмене случайно сгенерированным набором байт (nonce exchange) между клиентом и сервером с последующей выработкой единого сеансового секрета. Общая картина последовательности выполняемых запросов и ответов приведена ниже.

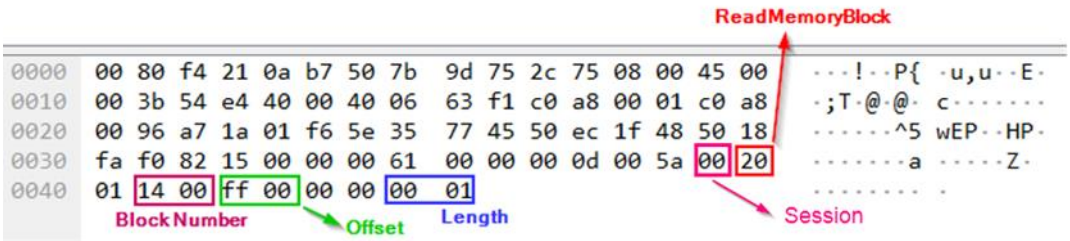
Процесс резервирования устройства при установленном Application Password



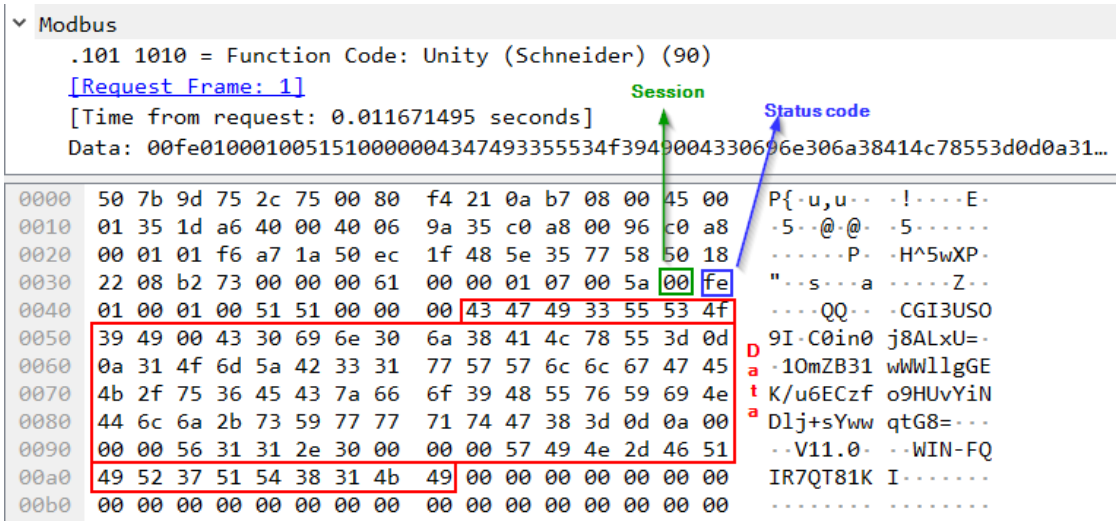
Давайте рассмотрим этот процесс немного подробнее.

После установления сеанса TCP программное обеспечение EcoStruxure™ Control Expert осуществляет запрос к ПЛК (порт 502/TCP) на чтение блока памяти с использованием UMAS функции 0x20, не требующей аутентификации.

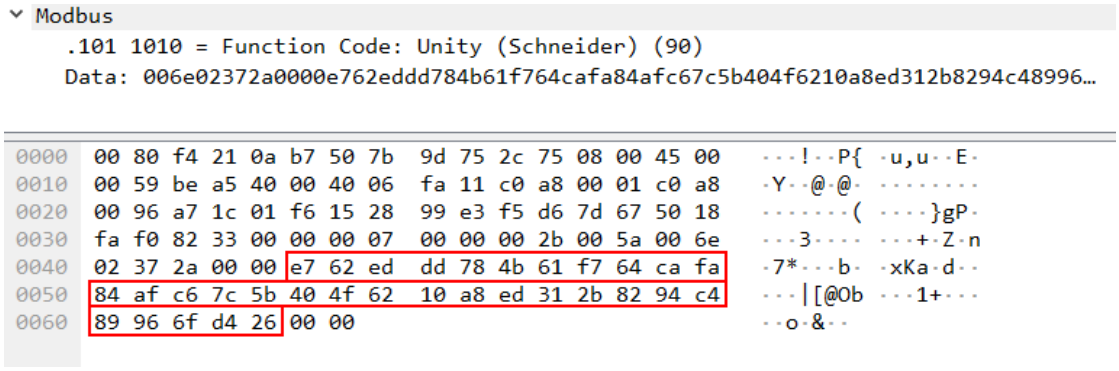
```
Modbus
    .101 1010 = Function Code: Unity (Schneider) (90)
    Data: 0020011400ff0000000001
```



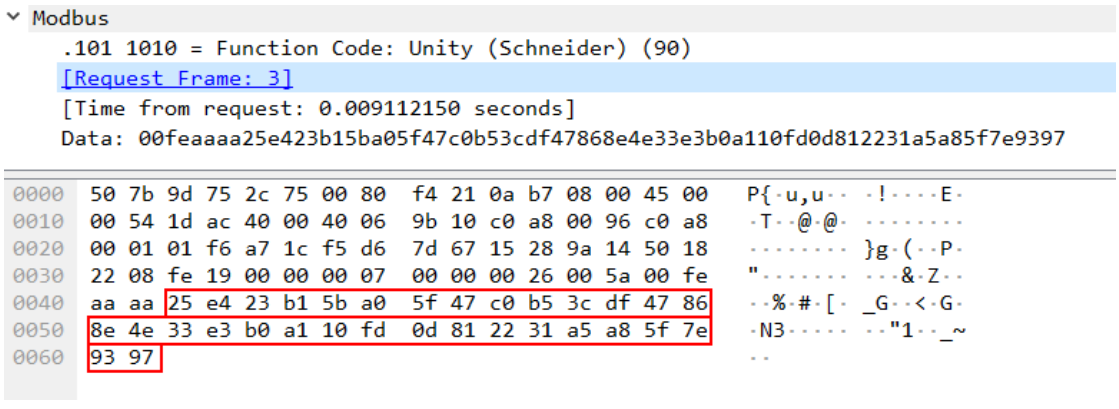
Далее клиент получает ответ от ПЛК. Данный блок памяти необходим для дальнейших вычислений, так как он содержит две base64 строки, которые являются хэшем пароля.



После этого EcoStruxure™ Control Expert генерирует и отправляет на ПЛК случайный набор байт (nonce) длиной 32 байта.



В ответ на полученный nonce ПЛК также отправляет EcoStruxure™ Control Expert набор байт (nonce response) длиной 32 байта.



При этом вычисленный на стороне ПЛК nonce response зависит только от предоставленного набора байт со стороны EcoStruxure™ Control Expert (nonce), в вычислениях данного случайного набора байт не используется

дополнительный случайный элемент. Другими словами, в ответ на один и тот же nonce всегда приходит один и тот же response.

На следующем шаге эти же nonce и response используются EcoStruxure™ Control Expert для вычисления SHA256-хэша, необходимого при резервировании ПЛК.

Вычисление хэша производится в соответствии со следующей схемой:

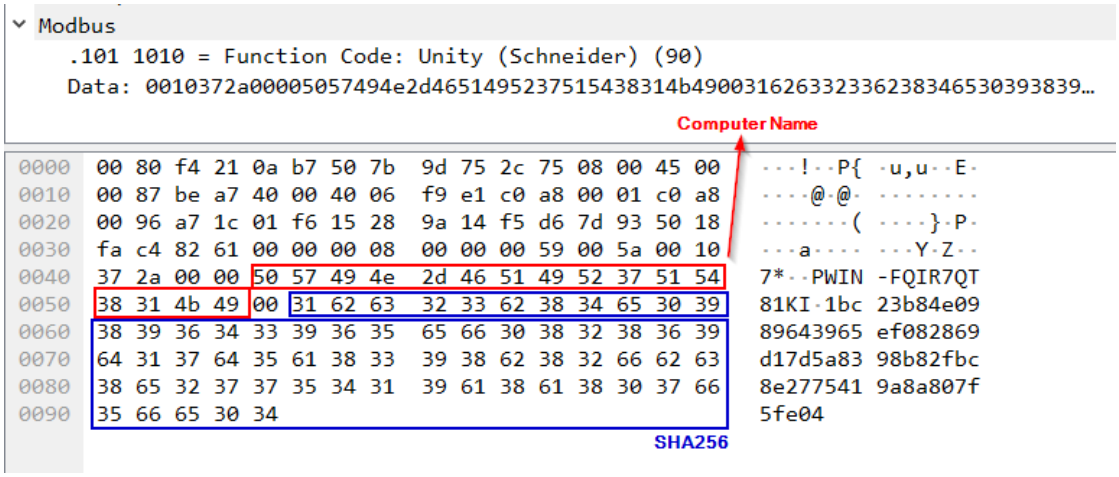
```
SHA256 (PLC nonce responce + base64 strings (password hash) from PLC's memory block + EcoStruxure Control Expert nonce)
```

Если использовать данные из приведенных выше примеров, то вычисление хэша будет выглядеть следующим образом:

```
SHA256("\x25\xe4\x23\xb1\x5b\xa0\x5f\x47\xc0\xb5\x3c\xdf\x47\x86\x8e\x4e\x33\xe3\xb0\xa1\x10\xfd\x0d\x81\x22\x31\xa5\xa8\x5f\x7e\x93\x97" + «\x43\x47\x49\x33\x55\x53\x4f\x39\x49\x00\x43\x30\x69\x6e\x30\x6a\x38\x41\x4c\x78\x55\x3d\x0d\x0a\x31\x4f\x6d\x5a\x42\x33\x31\x77\x57\x57\x6c\x6c\x67\x47\x45\x4b\x2f\x75\x36\x45\x43\x7a\x66\x6f\x39\x48\x55\x76\x59\x69\x4e\x44\x6c\x6a\x2b\x73\x59\x77\x77\x71\x74\x47\x38\x3d» + "\xe7\x62\xed\xdd\x78\x4b\x61\xf7\x64\xca\xfa\x84\xaf\xc6\x7c\x5b\x40\x4f\x62\x10\xa8\xed\x31\x2b\x82\x94\xc4\x89\x96\x6f\xd4\x26") = 1bc23b84e0989643965ef082869d17d5a8398b82fbc8e2775419a8a807f5fe04
```

В конечном итоге для резервирования ПЛК будут использованы имя компьютера, представленное символами ASCII, и вычисленный ранее SHA256 хэш.

```
PWIN-FQIR7QT81KI + '\x00' + 1bc23b84e0989643965ef082869d17d5a8398b82fbc8e2775419a8a807f5fe04
```



При успешном выполнении запроса сессия ПЛК вернет EcoStruxure™ Control Expert идентификатор сессии (`0xf8`).

```
Modbus
    .101 1010 = Function Code: Unity (Schneider) (90)
    [Request Frame: 5]
    [Time from request: 0.004372910 seconds]
    Data: 00fef8
```

```
0000  50 7b 9d 75 2c 75 00 80  f4 21 0a b7 08 00 45 00   P{·u,u·· ·!····E·
0010  00 33 1d ad 40 00 40 06  9b 30 c0 a8 00 96 c0 a8   ·3··@·@· ·0······
0020  00 01 01 f6 a7 1c f5 d6  7d 93 15 28 9a 73 50 18   ········ }··(·sP·
0030  22 08 46 53 00 00 00 08  00 00 00 05 00 5a 00 fe   "·FS···· ·····Z··
0040  f8                                                 ·
```

Впоследствии этот идентификатор сессии будет использоваться при отправке ПЛК защищенных команд Security function (`0x38`).

```
Modbus
    .101 1010 = Function Code: Unity (Schneider) (90)
    Data: f83801086c0a7e894ace8ddad9a6b80508c509a3fdf288fe551d40dab95b67d1d683d65a…
```

```
0000  00 80 f4 21 0a b7 50 7b  9d 75 2c 75 08 00 45 00   ···!··P{ ·u,u··E·
0010  00 58 be a9 40 00 40 06  fa 0e c0 a8 00 01 c0 a8   ·X··@·@· ········
0020  00 96 a7 1c 01 f6 15 28  9a 73 f5 d6 7d 9e 50 18   ·······( ·s··}·P·
0030  fa b9 82 32 00 00 00 09  00 00 00 2a 00 5a f8 38   ···2···· ···*·Z·8
0040  01 08 6c 0a 7e 89 4a ce  8d da d9 a6 b8 05 08 c5   ··l·~·J· ········
0050  09 a3 fd f2 88 fe 55 1d  40 da b9 5b 67 d1 d6 83   ······U· @··[g···
0060  d6 5a f8 41 ff 00                                 ·Z·A··
```

Как видно из приведенного выше анализа процесса резервирования ПЛК с использованием нового усовершенствованного механизма, данный метод абсолютно не является безопасным, так как все вычисления производятся на стороне клиента (EcoStruxure™ Control Expert), а «секрет» можно получить у ПЛК без аутентификации.

Также постоянный response от ПЛК при одном и том же nonce от клиента является дополнительным недостатком данного механизма, предоставляя злоумышленнику возможность Replay-атаки с помощью заранее собранного сетевого трафика процесса резервирования между легитимным клиентом (оператором) и сервером (ПЛК).

Обновленная процедура резервирования с использованием механизма Application Password

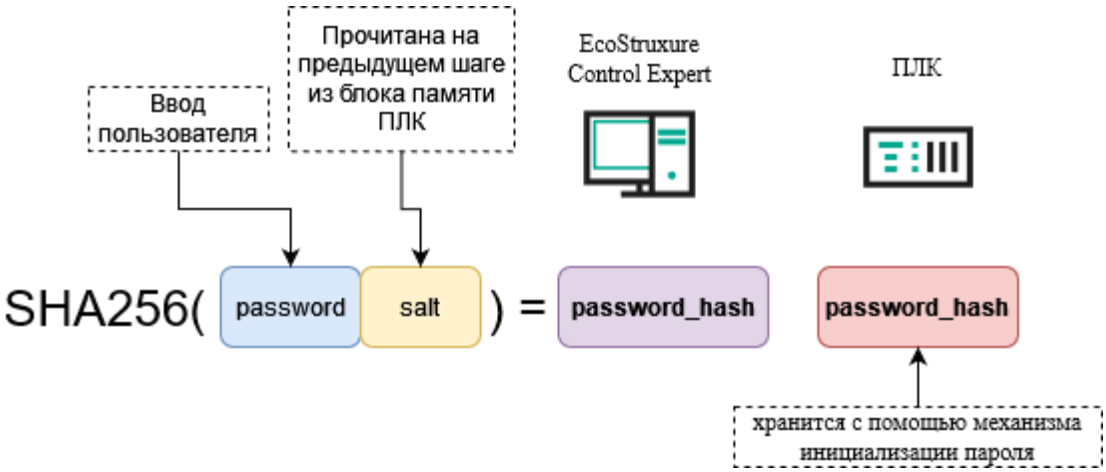
Ко времени публикации данной статьи Schneider Electric выпустил обновление для программного обеспечения EcoStruxure™ Control Expert (версия 15.1), ПЛК Modicon M340 (версия 3.50) и ПЛК Modicon M580 (версия 4.10). В этих обновлениях вендор исправил уязвимость, описанную в главе «Обход аутентификации с использованием механизма Application Password».

В данном разделе будет описана обновленная процедура резервирования ПЛК после обновления.

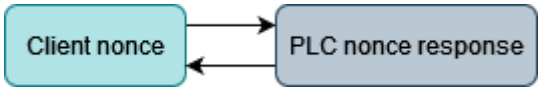
При резервировании ПЛК происходит чтение 0x534 байт блока памяти 0x14 с помощью двух запросов с использованием UMAS функции **pu_ReadMemoryBlock (0x20)**, которая не требует аутентификации. В предыдущей версии механизма резервирования в данном сегменте памяти находился хэш пароля, однако в новой версии там находится соль и некий шифротекст.

```
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 4b 6c 4e   ·····salt ····KlN
0130  33 6e 49 4c 4c 4e 4a 63  3d 0d 0a 0d 0a 00 00 00   3nILLNJc =·····
0140  61 54 70 70 62 35 74 6c  74 6a 49 54 41 44 55 55   aTppb5tl tjITADUU
0150  65 77 77 71 4e 76 6e 36  78 63 66 37 32 41 59 57   ewwqNvn6 xcf72AYW
0160  5a 45 30 69 56 79 58 61  32 43 63 47 6d 4d 7a 34   ZE0iVyXa 2CcGmMz4
0170  42 46 65 69 4e 32 62 6f  31 37 32 6f 6b 54 7a 7a   BFeiN2bo 172okTzz
0180  0d 0a 6e 37 54 79 38 48  36 53 51 35 71 50 6d 51   ··n7Ty8H 6SQ5qPmQ
0190  56 58 4f 55 4c 42 34 71  56 55 35 76 61 4c 79 57   VXOULB4q VU5vaLyW
01a0  63 51 51 7a 30 36 6a 79  6f 6d 36 74 49 6f 4a 67   cQQz06jy om6tIoJg
01b0  78 63 6d 31 6f 79 6e 2b  39 30 6d 76 7a 62 4c 30   xcm1oyn+ 90mvzbL0
01c0  58 59 0d 0a 4d 33 79 68  74 31 67 61 43 2f 67 35   XY··M3yh t1gaC/g5
01d0  2f 41 6e 42 72 35 61 6f  52 44 45 71 54 37 37 30   /AnBr5ao RDEqT770
01e0  61 44 37 38 4c 6d 72 79  6f 79 76 31 6f 69 4a 4e   aD78Lmry oyv1oiJN
01f0  54 31 38 4f 66 6c 73 54  38 65 51 6e 66 78 30 34   T18OflsT 8eQnfx04
0200  76 49 34 62 0d 0a 66 6b  2b 34 63 42 59 44 2f 6b   vI4b··fk +4cBYD/k
0210  50 56 6a 66 36 33 53 39  69 65 54 54 50 6e 79 77   PVjf63S9 ieTTPnyw
0220  64 30 65 51 70 6d 7a 67  53 49 46 71 79 50 5a 34   d0eQpmzg SIFqyPZ4
0230  67 75 51 33 2b 38 6f 2f  53 59 58 65 63 4e 71 32   guQ3+8o/ SYXecNq2
0240  51 33 63 4e 33 4f 0d 0a  45 4c 64 45 47 79 35 65   Q3cN3O·· ELdEGy5e
0250  31 36 34 46 69 6b 39 77  6a 75 6d 31 6b 51 58 6b   164Fik9w jum1kQXk
0260  42 53 76 56 4a 43 2b 6e  75 36 4a 37 6d 72 69 38   BSvVJC+n u6J7mri8
0270  61 43 69 78 53 39 6f 4d  73 68 6d 33 64 2b 32 70   aCixS9oM shm3d+2p
0280  5a 57 6b 4e 39 4a 52 52  0d 0a 67 64 71 54 35 75   ZWkN9JRR ··gdqT5u
0290  50 64 6d 4c 6e 48 31 51  7a 65 79 48 4d 58 7a 77   PdmLnH1Q zeyHMXzw
02a0  3d 3d 0d 0a 00 00 00 00  00 00 00 00 00 00 00 00   ==····· ········
02b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

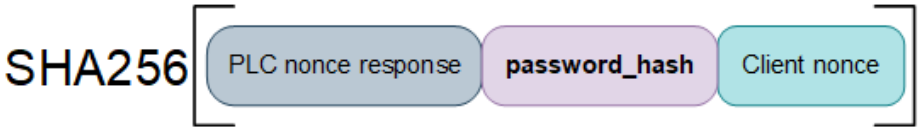
После того как клиент (EcoStruxure™ Control Expert) получает значение соли для хэширования, он может начать процедуру резервирования ПЛК. Клиент подсчитывает SHA256-хэш введённого пользователем пароля с полученной на предыдущем шаге солью для формирования хэша пароля.



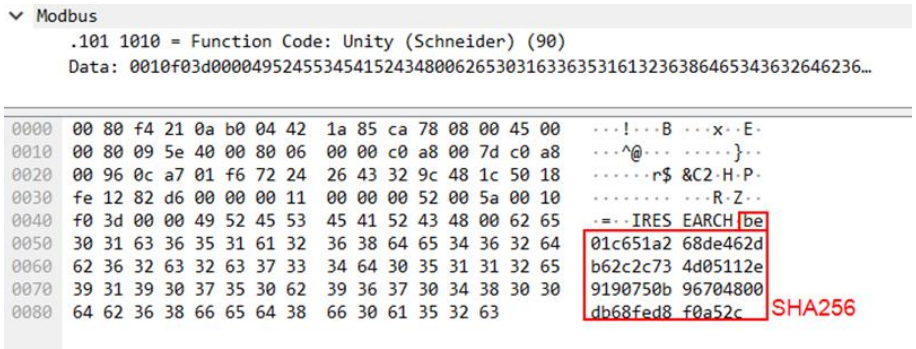
На следующем шаге происходит nonce exchange между клиентом и ПЛК.



На заключительном этапе клиент вычисляет SHA256 хэш, с помощью которого будет происходить резервирование устройства. Данный хэш состоит из PLC nonce, хэша пароля (password_hash) и Client nonce.



На скриншоте ниже показан запрос от клиента (EcoStruxure™ Control Expert) к ПЛК для совершения резервирования устройства с использованием подсчитанного SHA256 хэша.



В предыдущей версии механизма резервирования основной проблемой было то, что подсчёт «секрета» с помощью которого выполнялось резервирование устройства, происходил полностью на стороне клиента (EcoStruxure™ Control Expert). В исправленной реализации данного механизма в блоке памяти ПЛК 0x14 отсутствует хэш пароля, который участвует в формировании «секрета», т.е. финального SHA256 хэша.

Заключение

Как показал анализ, UMAS-протокол в реализации прошивки устройства Modicon M340 до версии 3.50 имеет существенные недостатки, которые критически влияют на безопасность систем автоматизации на основе решений Schneider Electric.

Согласно данным с shodan.io, количество доступных из глобальной сети устройств Modicon M340/M580 превышает 1000. Понятно, что это — лишь вершина айсберга.

Рекомендации вендора

Вендор рекомендует следовать мерам по устранению уязвимости обхода аутентификации для EcoStruxure™ Control Expert, описанным в advisory SEVD-2021-194-01, и использовать защитный механизм Application Password для полного устранения данной уязвимости.

Рекомендации Kaspersky ICS CERT

Kaspersky ICS CERT помимо предоставленных вендором рекомендаций также настоятельно советует производить мониторинг критически важных UMAS функций на уровне трафика — например, с помощью IDS, или используя специализированные решения для мониторинга сетевого трафика промышленной сети, выявления и анализа сетевых аномалий. Очевидно, что такие функции, как резервирование устройства, остановка работы устройства или загрузка/скачивание стратегии, являются критически важными, и атакующий с их помощью может нарушить технологический процесс.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com