Исследование безопасности: ThingsPro Suite – IIoT-шлюз и менеджер устройств от компании Moxa

Александр Ночвай

22.01.2019 Version 1.0

Оглавление

Описание объекта 3
Условия исследования 4
Результаты исследования 4
Этапы эксплуатации 5
Сложный путь 6
Простой путь 10
Фазы атаки 12
Остальные уязвимости 14
Итоги 14

Исследование безопасности технологий, которые используются разработчиками систем автоматизации и имеют потенциал применения на промышленных объектах по всему миру, является одним из приоритетных направлений работы Центра реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT).

Очевидно, что безопасность продуктов такого типа как IIoT требуют особого внимания. В этот раз объектом нашего исследования стал ThingsPro Suite – IIoT-шлюз и менеджер устройств от компании Moxa.

Важным аргументом в пользу нашего выбора послужил то факт, что использование ThingsPro Suite подразумевает удаленную доступность данного решения через сеть Интернет, так как ThingsPro Suite является решением для промышленных компьютеров – шлюзов Moxa UC-8100 Series – и имеет веб-интерфейс для управления своей платформой. Помимо этого, использование ThingsPro Suite подразумевает, что для передачи данных большинство устройств должны взаимодействовать с ним напрямую или через посредника, например, через другой шлюз.

Это означает, что ThingsPro Suite представляет собой точку выхода из индустриальной сети в интернет и наоборот – входную точку из сети Интернет в индустриальную сеть.

Описание объекта

Возможность повысить эффективность работы предприятия – главный аргумент, способствующий продвижению технологий промышленного интернета вещей в различных отраслях промышленного производства, сельском хозяйстве, транспорте, логистике, управлении городской инфраструктурой, коммунальном хозяйстве, энергетике. Перспективы, которые открывает применение этих технологий перед руководством компании, – действительно заманчивы. Это и централизованный мониторинг работы оборудования на удалённых объектах, позволяющий оценивать состояние износа и предсказывать, а значит, своевременно предотвращать поломки. И оптимизация работы удалённых промышленных объектов – предотвращение простоев, повышение эффективности расходования ресурсов, улучшение качества и увеличение количества выходной продукции.

Для реализации всех этих и многих других интересных возможностей современная концепция промышленного интернета вещей предполагает сбор данных от промышленных информационных систем – ПЛК, СКАДА, серверов OPC и непосредственно от «умного» полевого оборудования (датчиков и исполнительных механизмов) – и передачу данных в удалённую систему для их централизованной обработки а анализа. Как правило, при этом используются системы, развёрнутые в облаке (отсюда – слово «интернет» в названии концепции). По сути, речь идёт об ограниченной интеграции систем OT (Operational Technology) с удалёнными IT системами, доступными через интернет. Для упрощения и ускорения такой интеграции компания Moxa разрабатывает специализированное решение ThingsPro Suite.

ThingsPro Suite позиционируется как «коробочное решение», которое предназначено для сбора данных с компонентов OT и передачи собранных данных в облако третьей стороны, и как платформа для разработки своих собственных приложений по предобработке и анализу собранных данных.

ThingsPro Suite включает такую полезную функциональность, как сбор данных по протоколам Modbus TCP/RTU, передачу их в облако по протоколу MQTT, в том числе через 4G-сети, интеграцию с популярными облачными платформами MS Azure и Amazon. Администраторы системы получают удобную возможность для мониторинга состояния, конфигурирования и обновления установленных IIoT-шлюзов ThingsPro Gateway с возможностью отображения их на карте. В ThingsPro Suite реализована ролевая модель доступа и поддерживаются некоторые функции безопасности, такие как TLS v1.2 – шифрование и доступ через VPN.

Разработчикам приложений предоставлен C/Python API для предобработки и фильтрации данных, а также RESTful API для доступа ко встроенным функциям ThingsPro Suite.

Решение ThingsPro Suite предназначено для установки на промышленные компьютеры компании Moxa серии UC-8100

Компания Moxa сделала первый релиз ThingsPro Suite в 2017 году, и обновления выходят до сих пор. Мы исследовали ThingsPro Suite 2.1 Build 17072504.

Условия исследования

Изучив документацию, развернув демо-стенд и познакомившись с приложением ThingsPro Suite, мы выделили две недели на предварительное исследование с участием одного человека.

В качестве типа злоумышленника был выбран удаленный как наиболее распространенный и наиболее вероятный тип атакующего. Как следствие, мы решили начать исследования с проверки безопасности веб-сервиса – наиболее вероятной мишени атаки. Объектом исследования стало приложение веб-администрирования, которое работает на порту 80(HTTP) и 443(HTTPS).

Также стоит отметить, что наше исследование проходило методом «черного ящика»:

- Без консультаций с командой разработки компании Moxa;
- Без использования закрытой документации;
- Без изучения исходного кода.

Результаты были получены уже на предварительном этапе исследования.

Результаты исследования

В течение двух недель было обнаружено семь уязвимостей, среди которых есть максимально критичные — их эксплуатация приводит к исполнению произвольного кода в системе Linux. Также, совместная эксплуатация обнаруженных уязвимостей дает возможность удаленному злоумышленнику полностью захватить устройство и повысить привилегии до максимальных в системе без каких-либо изначальных данных аутентификации.

Необходимо отметить, что компания Moxa выпустила новую версию своего продукта – ThingsPro Suite 2.3, – в которой исправлены описанные ниже уязвимости. Более подробную информацию можно найти в подготовленном компанией Moxa бюллетене по безопасности.

Обнаруженным уязвимостям были присвоены следующие идентификаторы:

KLI D	CVE	Краткое описание уязвимости
KLCERT-18-018	CVE-2018-18390	User enumeration
KLCERT-18-019	CVE-2018-18391	User privilege escalation
KLCERT-18-020	CVE-2018-18392	Broken access control
KLCERT-18-021	CVE-2018-18393	The server side does not require the old password when changing the old password
KLCERT-18-022	CVE-2018-18394	Cleartext storage of sensitive information
KLCERT-18-023	CVE-2018-18395	Privilege escalation (hidden token) - 1 backdoor (10 CVSS)
KLCERT-18-024	CVE-2018-18396	Remote code execution - 1 RCE (10 CVSS)

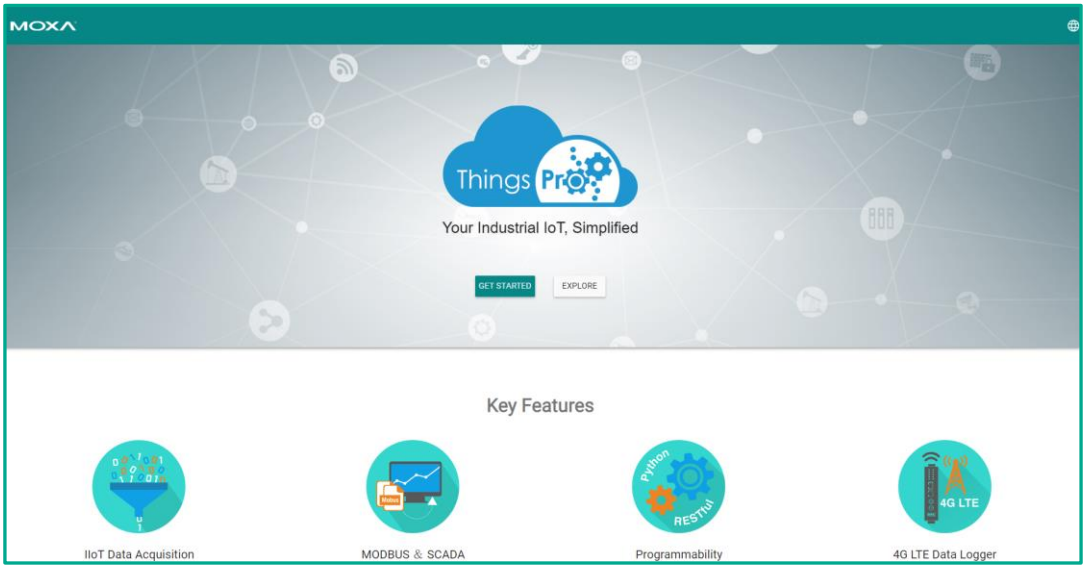
Далее в этой статье будет рассказано, что может сделать злоумышленник с ThingsPro Suite, эксплуатируя эти уязвимости.

На представленных ниже снимках экрана часть служебной информации отображена нечётко по просьбе компании Moxa.

Этапы эксплуатации

Прежде всего необходимо подчеркнуть, что эксплуатация обнаруженных нами уязвимостей возможна для злоумышленника, если тот имеет возможность отправлять запросы веб-серверу ThingsPro Suite и получать от него ответы или, проще говоря, может зайти на панель администрирования устройства. Только в этом случае у злоумышленника есть все условия для дальнейшей атаки на устройство.

Стартовая страница панели администрирования ThingsPro Suite



Мы разделили атаку на ThingsPro Suite через веб-сервис на четыре этапа получения привилегий в системе – от минимального уровня привилегий в веб-приложении до максимального в операционной системе.

1. Получение аутентификационных данных пользователя;
2. Повышение привилегий;
3. Выполнение произвольного кода;
4. Повышение привилегий в операционной системе.

Мы нашли два способа такой атаки – простой и сложный.

Начнем наше описание с более сложного способа эксплуатации уязвимостей.

Сложный путь

Получение аутентификационных данных пользователя

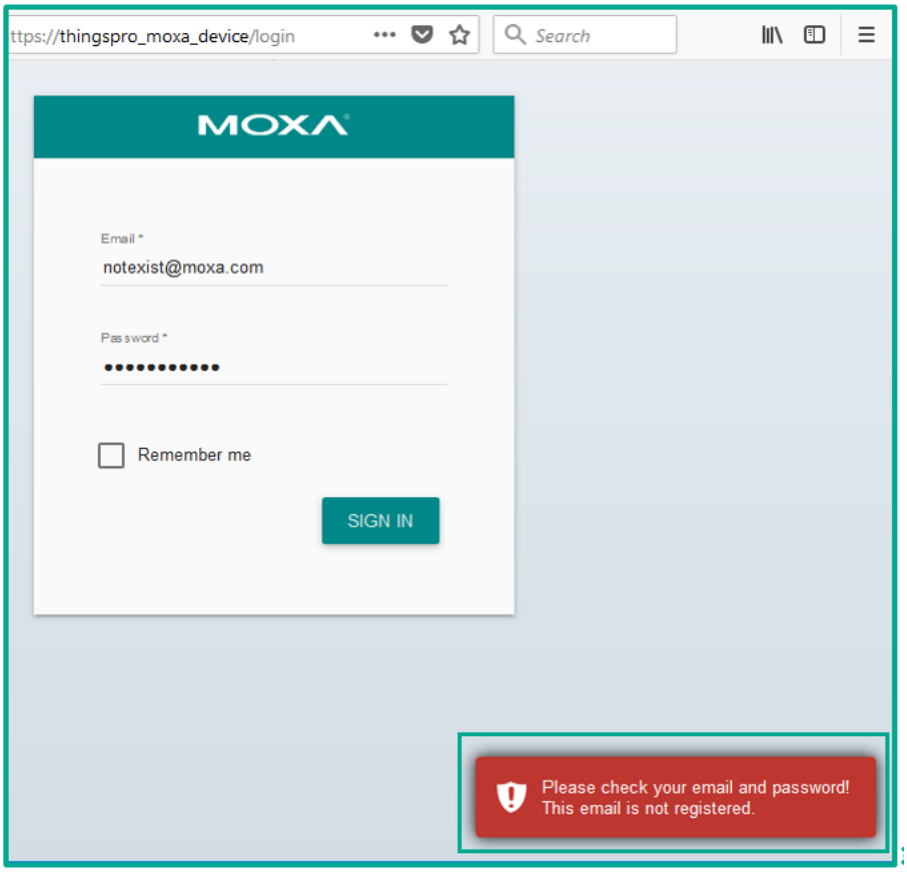
Сложный путь предполагает получение аутентификационных данных пользователя с помощью эксплуатации обнаруженной уязвимости KLCERT-18-018/CVE-2018-18390.

Поскольку панель администрирования ThingsPro Suite использует механизм аутентификации, злоумышленникам, чтобы получить авторизованный доступ к веб-интерфейсу, необходимы аутентификационные данные.

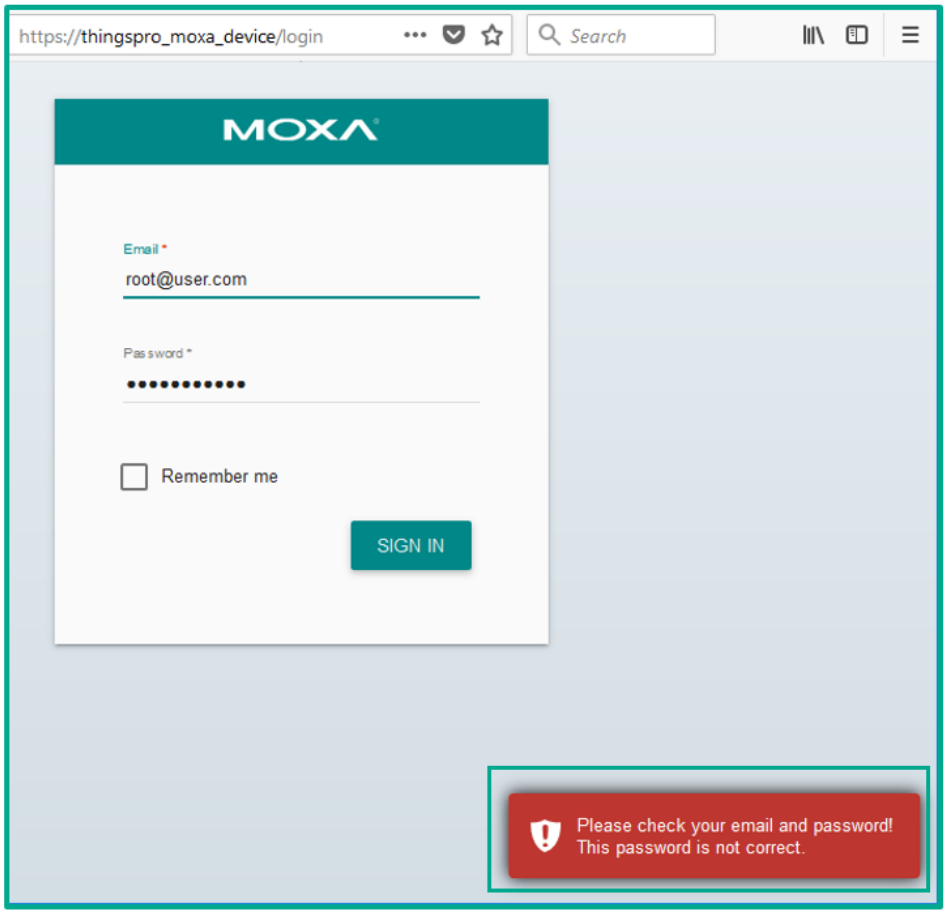
У злоумышленника есть возможность попробовать получить подтверждение того, что пользователь существует в системе. Эта уязвимость хорошо описана в OWASP-AT-002. Она заключается в том, что по ответам от сервера на полученные им данные аутентификации можно определить, существует пользователь в системе или нет.

Если пользователь указал имя пользователя, которого нет в системе, то сервер скажет об этом, вернув один ответ. Если же пользователь передал правильное имя пользователя, но неправильный для этого пользователя пароль, то сервер вернет уже другой ответ.

Пример эксплуатации уязвимости KLCERT-18-018/ CVE-2018-18390)



Пример эксплуатации уязвимости KLCERT-18-018/ CVE-2018-18390)



Таким образом злоумышленник может идентифицировать существующих в системе пользователей, перебрав их имена.

Если злоумышленник получит имя пользователя в системе, то это сильно облегчит ему получение пароля. Если же злоумышленник сможет подобрать и верный пароль для существующего пользователя, то следующим его шагом будет повышение привилегий в системе.

Повышение привилегий

После получения аутентификационных данных злоумышленнику необходимо повысить свои привилегии до максимальных в системе, потому что:

- Пользователю с привилегиями доступно больше возможностей в системе, чем другим пользователям;
- Атакующему с привилегиями доступно больше функционала, в котором могут содержаться уязвимости с другими последствиями.

Рассмотрим два способа повышения привилегий – через уязвимость KLCERT-18-019/CVE-2018-18391 и KLCERT-18-020/CVE-2018-18392.

Пример повышения привилегий через уязвимость KLCERT-18-019/CVE-2018-18391

Аутентифицированный пользователь ThingsPro Suite в веб-панели может изменять данные своего аккаунта. Среди этих данных – логин, пароль, адрес электронной почты и название компании. Для изменения этих данных веб-сервису отправляется HTTP-запрос, часть которого приведена ниже:

```
PUT /api/v1/users/{:id} HTTP/1.1
[...]

{"id":{:id},"name":"user","role":"user",
```

Из запроса видно, что помимо данных, указанных на странице веб-приложения, передается еще и текущая роль пользователя.

К нашему удивлению, после изменения значения role с user на root и повторной отправки сообщения, в ответе сервера было указано, что роль текущего пользователя изменена с user на root. Повторный вход в этот аккаунт подтвердил повышение привилегий до root. Данную уязвимость можно отнести к типу Broken Access Control, который занимает пятое место в рейтинге OWASP TOP 10 2017.

Пример повышение привилегий через уязвимость KLCERT-18-020/CVE-2018-18392

Во время исследования ThingsPro Suite оказалось, что аутентифицированный пользователь может изменять данные не только своего аккаунта, но и любого другого аккаунта в системе. Это очень полезно, если пользователю нужно изменить пароль для изначальных пользователей root или admin, если он его забудет.

Однако для злоумышленника это возможность повышения привилегий. Самым простым вариантом использования этой уязвимости может быть изменение произвольным пользователем с любым уровнем привилегий пароля для пользователя root. Фрагмент такого запроса, приведенный ниже, аналогичен предыдущему с той лишь разницей, что в теле указан идентификатор пользователя, равный единице, что соответствует пользователю с именем root.

```
PUT /api/v1/users/{:id} HTTP/1.1
[...]

{"id":{:id},"name":"user","role":"user",
```

Сервер, получив такой запрос, изменит пароль пользователя root на указанный в запросе и в дальнейшем атакующий может войти в систему как пользователь root.

Эта уязвимость также относится к типу Broken Access Control, который занимает пятое место в рейтинге OWASP TOP 10 2017.

Выполнение произвольного кода

Рассмотрим эксплуатацию уязвимости KLCERT-18-024/CVE-2018-18396.

Для пользователя с высоким уровнем привилегий в ThingsPro Suite доступна функциональность, которая изменяет системные настройки или поведение ThingsPro Suite в целом. Для обработки такого уровня запросов веб-приложение вынуждено обращаться к возможностям командной строки операционной системы Linux.

Один из таких запросов – это запрос на расширение RESTful API веб-приложения. (ThingsPro Suite позволяет расширять возможности веб-приложения, добавляя соответствующий обработчик.)

Обработчик этого запроса не проверяет полученные от пользователя данные на различные спецсимволы и сразу передает их на обработку в командную строку. Таким образом, манипулируя этими данными, злоумышленник вместе с командой, которую обычно вызывает веб-сервер ThingsPro для этого обработчика, может вызывать любую дополнительную команду из командной строки Linux.

Данная уязвимость относится к типу Injection, который в рейтинге OWASP TOP 10 2017 занимает первое место.

Фрагмент запроса для эксплуатации этой уязвимости показан ниже:

```
POST /api/v1/market/upload HTTP/1.1
[...]
Content-Type: multipart/form-data; boundary=--------886584073
----------886584073
Content-Disposition: form-data; name="file"; filename="
"
----------886584073—
```

Повышение привилегий внутри системы

Как правило, для развития атаки на веб-сервер после получения доступа к командной оболочке Linux требуется повышение привилегий, потому что обычно веб-серверы запускаются из-под отдельно созданного в системе пользователя с ограниченными правами. Так работает, например, apache или nginx. Однако, веб-сервер ThingsPro Suite уже запущен из-под пользователя root в системе, поэтому, получив возможности выполнения произвольных команд, злоумышленнику повышать привилегии не надо.

Ниже приведен вывод результата команды id, которая отображает полученный после эксплуатации уязвимости уровень текущих привилегий пользователя в системе Linux.

```
$ ncat -nklvp 8080
Ncat: Version 7.40 ( https://nmap.org/ncat )
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from .
Ncat: Connection from :.
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
uname -a
Linux  Thu Apr 20 15:22:58
```

Значения uid, gid и groups, равные нулю, означают наличие максимальных привилегий в системе у пользователя, который запустил команду id.

Данная слабость является существенным недостатком для всего устройства в целом.

Ограничения в эксплуатации

Описанный Сложный путь получения привилегий подразумевал, что атакующему для успешного прохождения системы аутентификации необходимо:

1. Подобрать логин существующего пользователя в системе;
2. Подобрать пароль для обнаруженного логина.

Эти действия не всегда могут быть выполнены – например, в тех случаях, когда для пользователей были установлены очень сложные пароли, или атакующий оказался недостаточно удачлив. Тогда атакующему приходится искать другие пути для проникновения в веб-приложение.

Одним из таких путей может стать эксплуатация обнаруженной уязвимости KLCERT-18-023/CVE-2018-18395.

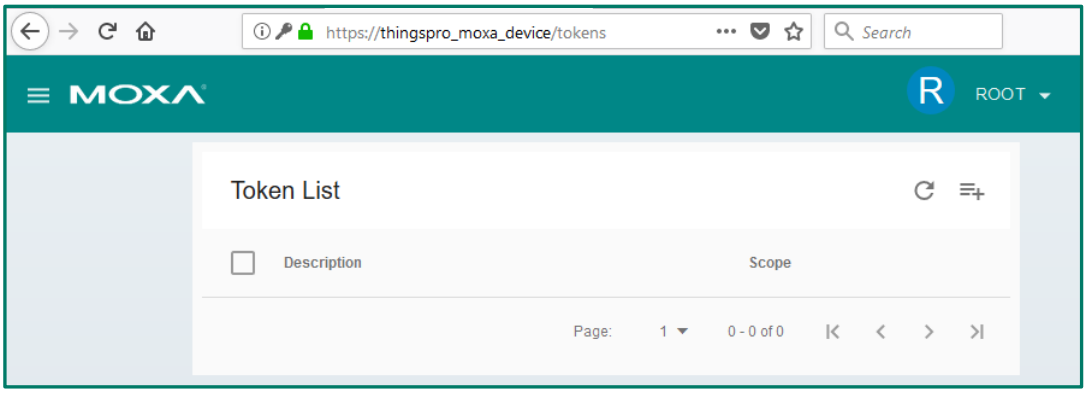
Простой путь

Получение аутентификационных данных пользователя

Простой путь предполагает получение аутентификационных данных пользователя с помощью эксплуатации обнаруженной уязвимости KLCERT-18-023/CVE-2018-18395.

Уязвимость заключается в том, что веб-сервер ThingsPro Suite содержит в себе «спрятанный» токен для RESTful API. Визуально веб-интерфейс не отображает этот токен в списке созданных токенов, в том числе и для пользователя с root-привилегиями, то есть максимальными. Это показано ниже:

Отображение в панели веб-администрирования пред-установленных токенов



Такое поведение существует из-за того, что обработчик запроса на список получения токенов для этой вкладки фильтрует все токены из базы данных, если для них установлен положительный параметр hidden, и не выводит их на веб-интерфейс.

Ниже представлен запрос из базы данных на вывод всех существующих токенов:

```
$ ncat -nklvp 8080
Ncat: Version 7.40 ( https://nmap.org/ncat )
Ncat: Listening on :::8080
Ncat: Listening on 0.0.0.0:8080
Ncat: Connection from [redacted].
Ncat: Connection from [redacted].
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
uname -a
Linux [redacted] Thu Apr 20 15:22:58 [redacted]
```

Несмотря на то, что, согласно описанию, «спрятанный» токен является «Internal Local Token», им может воспользоваться и внешний злоумышленник.

Повышение привилегий

ThingsPro Suite использует токены двух типов – read и write. Токен типа «write» способен на те же действия, что и пользователь с привилегиями уровня «root» в веб-приложении. Токен типа «read» является пользователем с привилегиями «user».

«Спрятанный» токен является токеном типа «write», поэтому, используя его, повышать привилегии нет необходимости.

Выполнение произвольного кода

При наличии «спрятанного» токена и, как следствие, максимальных привилегий в веб-приложении, и поиск уязвимостей, и алгоритм эксплуатации уязвимости, приводящей к выполнению произвольного кода, становится аналогичным описанному выше в части «Сложный путьь» – с той лишь разницей, что в заголовках запроса будет использоваться «спрятанный» токен вместо сессии.

Повышение привилегий внутри системы

С наличием возможности выполнения произвольного кода в системе и при наличии токена алгоритм повышения привилегий в системе аналогичен описанному выше в части «Сложный путьь».

Ограничения в эксплуатации

Описанный простой путь эксплуатации подразумевал, что атакующему для успешного прохождения системы аутентификации необходимо знать значение «спрятанного» токена.

Само же значение «спрятанного» токена генерируется при первом запуске веб–приложения и представляет собой результат выполнения хеш-функции bcrypt для десяти псевдослучайных символов. Это означает, что атакой типа bruteforce это значение будет сложно подобрать, однако, если будет получен seed, который использовался для получения десяти псевдослучайных символов, то возможно будет восстановить эти десять символов, а на основе их сгенерировать заново токен.

Другой возможный вариант получения значения «спрятанного» токена – извлечение из файловой системы: ThingsPro Suite сохраняет это значение по статическому пути в файле и в качестве записи в базе данных.

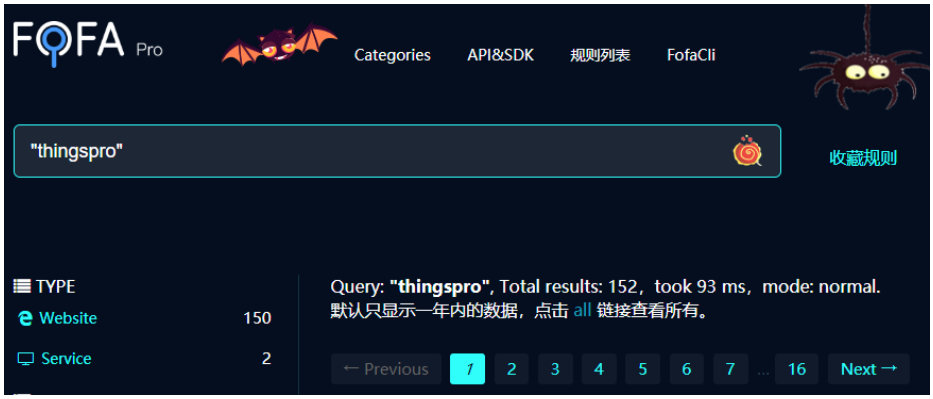
Фазы атаки

Обнаружение

На сегодняшний день существуют такие платформы, как shodan.io и fofa.so. Обе эти платформы занимаются тем, что сканируют диапазоны сетей на наличие открытых сетевых сервисов, что упрощает обнаружение доступных IP-адресов ThingsPro Suite.

Таким образом, например, в начале ноября 2018 года shodan.io выдал 43 IP-адреса, сервисы которых возвращают строку “thingspro” на сетевой запрос. Платформа fofa.so возвращает результат с уже 152 упоминаниями “thingspro”. Эти результаты показаны ниже:

Результаты поиска ThingsPro Suite с помощью Shodan и Fofa



Идентификация версии

Некоторые злоумышленники пропускают этап идентификации версии атакуемого программного обеспечения и сразу переходят к этапу эксплуатации. Во время проведения тестирования на проникновения нам также иногда приходится прибегать к подобному способу, однако, успешное прохождение этого этапа повышает шансы на успешную эксплуатацию уязвимости в дальнейшем.

Помимо основного веб-сервиса на портах 443 и 80, предоставляющего панель администрирования, веб-сервер ThingsPro Suite открывает еще один веб-сервис на порту 8880. При обращении на этот порт по HTTP, веб-сервис возвращает статичную страницу на языке XML, в которой содержится следующая информация:

- Версия ThingsPro Suite;
- Mac-адрес;
- IP-адрес.

Основная проблема веб-сервиса, открытого на порту 8880, заключается в том, что у него отсутствует механизм аутентификации. То есть информация, которая позволит однозначно определить, какая версия ThingsPro Suite используется и является ли она уязвимой, может быть получена любым участником сети интернет.

Пример такого ответа от веб-сервиса на порту 8880 представлен ниже:

Пример ответа от веб-сервиса на порту 8880

Эксплуатация

Следующим этапом после обнаружения веб-сервиса ThingsPro Suite и идентификации его версии является этап эксплуатации уязвимостей, который полностью описан в предыдущей главе. Остается лишь напомнить о том, что последовательная эксплуатация двух уязвимостей приводит к тому, что злоумышленник, имеющий только возможность обращаться к основному веб-сервису ThingsPro Suite, может получить доступ к командной строке Linux на сервере ThingsPro Suite с привилегиями root-пользователя.

Остальные уязвимости

Помимо упомянутых выше пяти уязвимостей, во время исследования были обнаружены еще две, которые могут не использоваться в описанной выше атаке, однако о них тоже необходимо сказать.

Обнаруженная уязвимость KLCERT-18-021/CVE-2018-18393 является слабостью парольной политики. Она заключается в том, что пользователю для изменения своего пароля не нужно вводить предыдущий пароль. Можно предположить, что если бы такой уязвимости в ThingsPro Suite не было, то один из векторов эксплуатации обнаруженной уязвимости KLCERT-18-020/CVE-2018-18392 (Broken Access control) по изменению пароля для пользователя root (использовался для повышения привилегий) был бы неприменим.

Обнаруженная уязвимость KLCERT-18-022/CVE-2018-18394 является подходящей для пост-эксплуатации уязвимостей типа SQL-инъекции. Уязвимость заключается в том, что ThingsPro Suite хранит чувствительные данные в своей базе данных в открытом виде. Среди этих чувствительных данных есть информация о сгенерированных и «спрятанном» токене. Таким образом, несмотря на то, что пароли пользователей в базе данных хранятся в хешированном виде, злоумышленник может попытаться извлечь токены и использовать уже их в качестве данных аутентификации, тем самым избавившись от нужды дехеширования паролей.

Итоги

К концу 2017 года нами было обнаружено 7 уязвимостей в продукте ThingsPro Suite от компании Moxa. Среди этих уязвимостей были уязвимости, оцененные в 10 баллов по шкале CVSS v3.0. Последовательная эксплуатация двух уязвимостей приводит к тому, что удаленный злоумышленник, который имеет только доступ к веб-приложению ThingsPro Suite, может получить доступ к командной строке операционной системы, где запущен ThingsPro Suite. Эксплуатация этих уязвимостей может быть автоматизирована для массовой атаки на устройства ThingsPro.

При этом большинство найденных уязвимостей были обнаружены в кратчайший промежуток времени без глубокого технического анализа и без анализа исходного кода веб-приложения. Это говорит о том, что данные уязвимости могут быть обнаружены и проэксплуатированы злоумышленником, который не обладает высоким уровнем технических навыков.

Обо всех уязвимостях, обнаруженных нами в программном обеспечении компании Moxa, мы сообщили производителю ПО.

В настоящее время все уязвимости исправлены:

- В декабре 2017 года были начаты исследования.
- В январе 2018 года был написан отчет и передан группе безопасности компании Moxa.
- В конце июля 2018 года компания Moxa выпустила патч.
- В октябре 2018 года был выпущен бюллетень по безопасности.
- В октябре 2018 года были опубликованы описания уязвимостей.

Мы благодарим за сотрудничество компанию Moxa. Сотрудники службы безопасности компании действовали профессионально и с большим желанием решить проблемы своего продукта. Отметим также прозрачность в переговорах с представителями компании и их быстрые ответы.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab 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 lab ICS CERT ics-cert@laspersky.com