Уязвимости в промышленных решениях 2018\2019

Валерия Кривко
Руководитель Пресейл Службы
2019

KASPERSKY lab

Почему промышленные компании легко атаковать?

Очень легкие и словарные пароли

Недостатки сегментации сетей и фильтрации трафика(отсутствие ДМЗ между КИС и ТС)

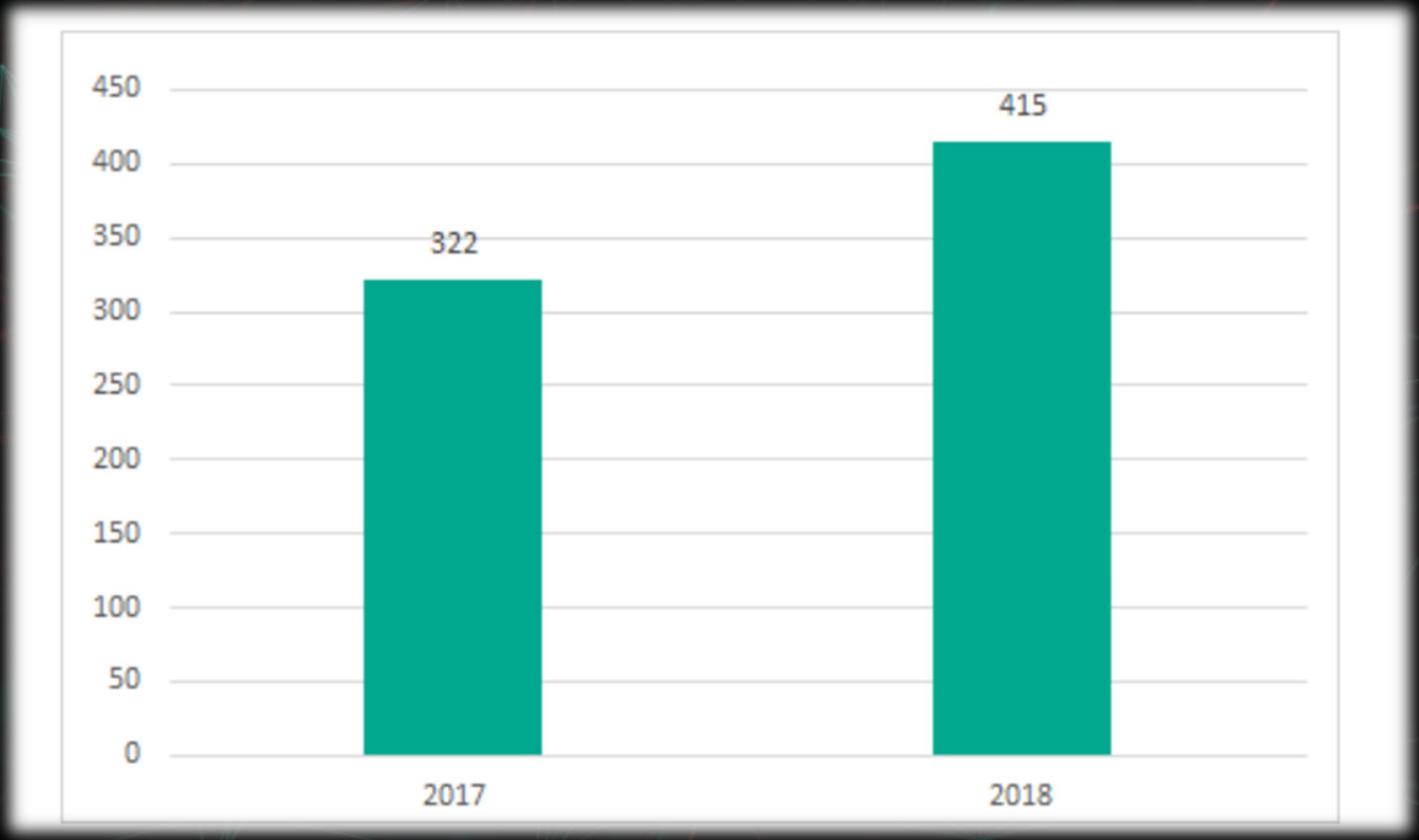
Использование выделенного канала в обход ДМЗ

Избыточные привилегии пользователей и ПО

Сохранные параметры аутентификации для доступа к критически важным системам

Использования одинаковых паролей к различным системам

Количество обнаруженных уязвимостей



KASPERSKY lab

Уязвимые компоненты АСУ ТП

Наибольшее количество уязвимостей было выявлено в:

- Инженерном ПО
- SCADA/HMI-компонентах
- Сетевых устройствах промышленного назначения
- ПЛК

14 уязвимостей в системе SafeNet Sentinel, разработанной компанией Gemalto

Уязвимости в промышленных компьютерах и серверах

Уязвимости в решениях по защите промышленных сетей

В устройствах безопасности Allen-Bradley Stratix 5950 обнаружены опасные уязвимости

SECURITYLAB.RU 5 июля 2018

КОММЕНТАРИИ

В средствах сетевой защиты для промышленных сетей Allen-Bradley Stratix 5950 от компании Rockwell Automation обнаружены множественные уязвимости, с помощью которых злоумышленник может обойти клиентские сертификаты и подключиться к уязвимому устройству или вызвать сбой в его работе.

Проблемы связаны с использованием операционной системы Cisco Adaptive Security Appliance (ASA). Уязвимости затрагивают модели Allen-Bradley Stratix 5950, работающие под управлением Cisco ASA 9.6.2 и более ранних версий: 783-SAD4T0SBK9, 1783-SAD4T0SPK9, 1783-SAD2T2SBK9 и 1783-SAD2T2SPK9.

KASPERSKY lab

Schneider Electric

SecurityLab.ru by Positive Technologies

Новости | Уязвимости | Статьи | Софт | Блоги | PHDays

Главная / Новости

14:12 / 21 Ноября, 2018

В ПЛК Schneider Electric выявлена опасная уязвимость

Теги: Schneider Electric, ПЛК, уязвимость, АСУ ТП

Проблема позволяет изменить параметры настроек IPv4 и перехватить трафик целевого устройства.

В программируемых логических контроллерах производства компании Schneider Electric выявлена опасная уязвимость, позволяющая изменить конфигурацию IPv4 (IP-адрес, маску подсети, шлюз) при удаленном подключении к устройству.

Уязвимость (CVE-2018-7798) существует в результате некорректной реализации сетевого модуля в протоколе UMAS, что предоставляет атакующему возможность перехватить трафик целевого ПЛК путем удаленной модификации параметров конфигурации. Проблема затрагивает ПЛК серии Modicon M221 (все версии). Степень опасности уязвимости оценена в 8,2 балла по классификации CVSS v3.

09:31 / 7 Сентября, 2018

Schneider Electric поставляла зараженные «флешки» вместе со своими продуктами

Теги: Schneider Electric, вредоносное ПО, SCADA

«Проблемные» накопители поставлялись со всеми версиями Conext ComBox и Conext Battery Monitor.

Французская энергомашиностроительная компания Schneider Electric призналасьь , что некоторые съемные USB-накопители, поставляемые вместе с продуктами Conext ComBox и Conext Battery Monitor, инфицированы вредоносным ПО. Согласно заявлению компании, «флешки» оказались заражены в процессе производства на предприятии стороннего поставщика.

«Проблемные» накопители поставлялись со всеми версиями Conext ComBox (sku 865-1058) и Conext Battery Monitor (sku 865-1080-01).

По заверениям компании, накопители содержат пользовательскую документацию и ряд несущественных программ и не хранят программное обеспечение, требуемое для

10:27 / 29 Августа, 2018

В оборудовании Schneider Electric обнаружены опасные уязвимости

Теги: Schneider Electric, уязвимость

Одна из уязвимостей является критической и позволяет злоумышленнику удаленно выполнить код.

В промышленном оборудовании от компании Schneider Electric обнаружены пять опасных уязвимостей, одна из которых критическая.

Первая уязвимость CVE-2018-7795 представляет собой проблему некорректной проверки входных данных во время генерации web-страницы и является критической. Успешная эксплуатация данной уязвимости может привести к манипулированию данными, позволяя злоумышленнику удаленно выполнить код. Проблема затрагивает измеритель мощности PowerLogic PM5560 с версией прошивки 2.5.4 и более ранними.

Вторая уязвимость CVE-2018-7789 обнаружена в логическом контроллере Modicon M221 с версией прошивки 1.6.2.0. Проблема может позволить неавторизованному пользователю удаленно перезагрузить устройство.

08:49 13 декабря, 2017

«Транснефть» отказалась от использования продуктов Schneider Electric

Теги: Транснефть, АСУ ТП, Schneider Electric

Российская компания не удовлетворена состоянием кибербезопасности своих АСУ ТП.

Российский оператор магистральных нефтепроводов «Транснефть» больше не будет использовать оборудование производства Schneider Electric. Причиной являются многочисленные уязвимости, ставящие под угрозу кибербезопасность компании. Решение было озвучено первым вице-президентом «Транснефти» Максимом Гришаниным на заседании экспертного совета по кибербезопасности, сообщает ТАСС.

Как пояснил Гришанин, в прошлом и нынешнем году его компания сделала глубокий анализ рисков для своих АСУ ТП. В ходе проверки были выявлены многочисленные критические уязвимости, в том числе во встроенных механизмах защиты АСУ ТП. Специалисты уведомили производителя об обнаруженных проблемах с безопасностью, однако ответа пришлось ждать очень долго. «Транснефть» реализует программу импортозамещения, и вместо Schneider Electric будут использоваться отечественные аналоги.

10:59 / 16 Мая, 2018

В ПЛК Siemens SIMATIC S7-400 обнаружена серьезная уязвимость

Теги: Siemens, SIMATIC, уязвимость, отказ в обслуживании

Устройства не могут правильно проверять пакеты S7, позволяя удаленному злоумышленнику добиться отказа в обслуживании.

Компания Siemens сообщила об обнаружении в ряде программируемых логических контроллеров SIMATIC S7-400 серьезной уязвимости CVE-2018-4850, позволяющей добиться отказа в обслуживании.

SIMATIC S7-400 представляет собой семейство программируемых логических контроллеров (ПЛК), предназначенных для управления технологическими процессами в промышленности. Продукт используется во всем мире в области автомобилестроения, производства механического оборудования, строительства, производства стали, производства и распределения электроэнергии, химического, складского, пищевого и фармацевтического секторов.

По словам представителей Siemens, данные устройства не проводят корректную проверку пакетов S7, позволяя удаленному злоумышленнику добиться отказа в обслуживании, заставив систему войти в режим DEFECT и оставаться в нем, пока она не будет

13:24 / 19 Апреля 2019

Атака была протестирована на 16 устройствах от 6 различных производителей, в частности, ABB, Phoenix Contact, Schneider Electric, Siemens и WAGO. По мере возможности она производилась на ПЛК с установленными по умолчанию настройками.

«ПЛК реагировали по-разному: одни полностью перестали обновлять состояние входов, работа других существенно замедлилась», - отметили специалисты.

Только одно из протестированных устройств оказалось не подвержено атаке данного типа. Стоит отметить, что патчи, устраняющие данную уязвимость, выпустил только 1 вендор из шести. В частности, компания Schneider Electric выпустила соответствующие обновления для решений Modicon M221 и EcoStruxure Machine Expert. В ABB заявили, что атака затрагивает только устройства с установленными по умолчанию настройками. По словам представителей Phoenix Contact, проблема касается только устаревших устройств и не затрагивает новые версии продуктов. Как сообщили в Siemens, ее продукты уязвимости не подвержены, а в WAGO заявили, что проблема довольно старая и порекомендовали предпринять меры против ее эксплуатации, в частности, использовать ПЛК в закрытых сетях либо защитить их межсетевым экраном, а также установить ограничение сетевого трафика.

АСУ ТП и ИБ – параллельные миры

Уязвимость, да и ладно …

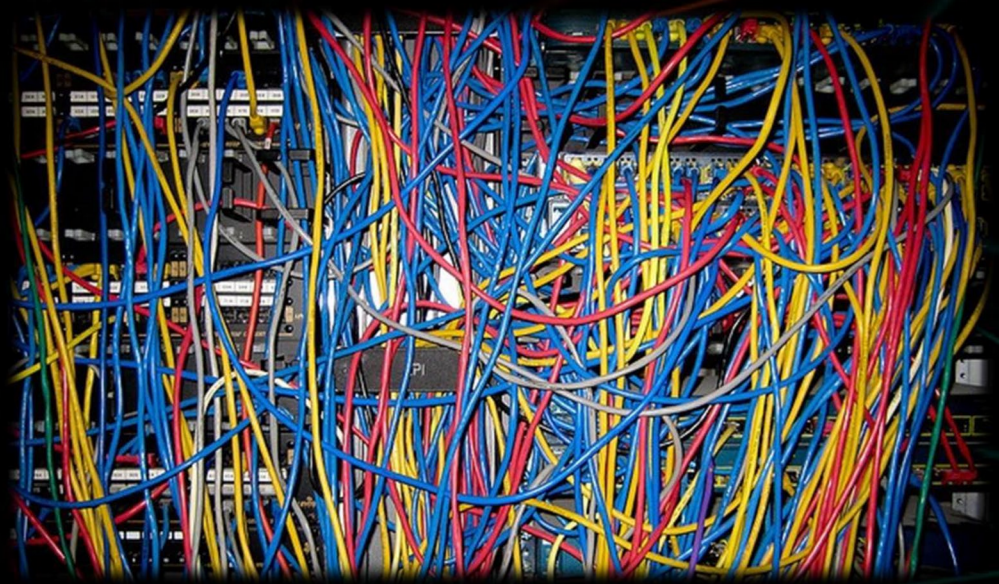
Вендоры АСУ ТП не хотят исправлять уязвимости

ИБ не понимают инженеров

Инженеры не понимают ИБ

Работает – не трогай!

Непонятно, кто отвечает за ИБ АСУ ТП



Что делать?

Иметь на заводе отдельную службу, отвечающую за безопасность и внутренний аудит инфраструктуры АСУ ТП

Громко проявлять недовольство и давить на вендоров, заставляя их исправлять уязвимости

Проводить внешние аудиты защищенности инфраструктуры АСУ ТП

Создать мотивацию и заставить владельцев критичных объектов АСУ ТП заниматься их безопасностью


WE PROTECT WHAT MATTERS MOST
KASPERSKY lab