

РАЗРАБОТКА СЦЕНАРИЕВ АТАК НА ПАНЕЛЬ ОПЕРАТОРА В АСУ ТП

Устинов С.А., Лазарев Т.П., студенты 5 курса факультета безопасности

Научный руководитель – Новохрестов А.К., кандидат технических наук, доцент

ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники»

***Ключевые слова:** Панель оператора, АСУ ТП, уязвимости, протокол Modbus TCP/IP, база данных CVE, сценарии атак.*

Исследование фокусируется на проблемах безопасности АСУ ТП, освещается опасность атак, направленных на панель оператора. В ходе работы проведен анализ уязвимого компонента и возможных уязвимостей. Также предложены сценарии атак, в рамках которых эксплуатировалась уязвимость протокола Modbus TCP/IP.

Введение. Сегодня, когда информационные технологии интегрируются во все аспекты нашей повседневной жизни, обеспечение безопасности автоматизированных систем управления технологическим процессом (АСУ ТП) становится критической задачей. Одним из наиболее опасных методов атаки на АСУ ТП является воздействие на программируемые логические контроллеры (ПЛК) [1]. В данном исследовании атака на АСУ ТП рассматривается со стороны вмешательства злоумышленника в работу ПЛК через панель оператора.

Цель работы. В ходе работе был определен следующий сценарий атаки злоумышленника: первым этапом нарушитель направляет свои усилия на ПЛК, затем, после успешного вторжения, осуществляет атаку на панель оператора. В процессе изучения взаимосвязей между ПЛК и панелью оператора был выделен протокол, уязвимость которого подлежит эксплуатации – а именно, протокол Modbus TCP/IP [2].

Для разработки сценариев атак на панель оператора, был проведен поиск подходящих для нашего случая уязвимостей, который осуществлялся в базе данных CVE [3].

Результаты исследования. Так как в разрабатываемом сценарии атаки будут эксплуатироваться уязвимости протокола Modbus, при поиске было введено ключевое слово «Modbus». В результате выполнения поискового запроса был получен список из 128 уязвимостей.

Для дальнейшей работы было решено брать CVE не раньше 2018 года. Также было необходимо, чтобы уязвимость эксплуатировалась конкретно в Modbus TCP/IP, а не, например, в сервере Modbus. Кроме того, смотрелось, каким образом можно реализовать выбранную уязвимость (возможно ли это сделать, работая с ПЛК и панелью оператора). После проведенного анализа были отобраны 23 уязвимости, часть из которых представлена в таблице 1.

Таблица 1 - Отобранные уязвимости

Уязвимость	Описание
1. CVE-2022-4856	Переполнение буфера, которое ведёт к обходу аутентификации
3. CVE-2019-6527	Изменение пароля пользователя-администратора
4. CVE-2018-7846	Получение несанкционированного доступа путём брутфорса по протоколу Modbus на контроллере
5. CVE-2022-24323	Перехват и манипуляция данными ответа Modbus
7. CVE-2023-25619	Отказ в обслуживании контроллера при обмене данными по протоколу Modbus TCP
...	...
21. CVE-2022-1068	Переполнение буфера, которое ведёт к сбою программ
22. CVE-2018-4838	Понижение или обновление прошивки (версии) устройства
23. CVE-2021-22786	Раскрытие конфиденциальной информации при обмене данными по протоколу Modbus TCP

Для составления отдельных сценариев атак смотрелось, на что или через что эксплуатируется каждая уязвимость. Это делалось для того, чтобы все уязвимости в разработанном сценарии атаки были нацелены на одно и то же уязвимое ПО или уязвимый компонент. Так на основе отобранных уязвимостей было разработано четыре сценария атак (таблица 2).

Таблица 2 - Разработанные сценарии атак

Сценарий	Уязвимости	Описание
№1	CVE-2022-45789 CVE-2021-22786 CVE-2021-22779	1) Перехват аутентифицированного сеанса; 2) Получение доступа к конфиденциальным данным, хранящимся в памяти контроллера; 3) Получение возможности вносить изменения в данные, передаваемые по протоколу Modbus TCP.
№2	CVE-2018-4838 CVE-2022-37300 CVE-2022-24323	1) Понижение версии EcoStruxure Process Expert до более старой, обладающей уязвимостями; 2) Получение доступа к контроллеру; 3) Перехват и манипуляция данными ответа протокола Modbus.
№3	CVE-2018-4840 CVE-2022-24322 CVE-2023-25619	1) Загрузка изменённой конфигурации системы с изменением паролей для авторизации; 2) Перехват и манипуляция данными ответа протокола Modbus; 3) Отказ в обслуживании контроллера при обмене данными по протоколу Modbus TCP.
№4	CVE-2018-7846 CVE-2021-22786 CVE-2019-6807	1) Получение доступа к контроллеру; 2) Считывание конфиденциальных данных; 3) Сбой системы.

Заключение. При разработке данных сценариев была определена общая структура сценария атаки, то есть все четыре разработанных сценария атаки имеют один и тот же шаблон. В данной структуре у злоумышленника есть два действия, которые он выполняет для достижения своих целей. Первое действие - это обход аутентификации для проникновения в систему. Второе действие - это перехват конфиденциальной информации, а также манипуляция этими данными.

Данная структура сохраняется в каждом разработанном сценарии, меняются только пути достижения целей, а также последствия выполнения указанных выше действий. Также следует отметить, что в сценариях используется тип атаки man-in-the-middle.

Таким образом, в результате исследования удалось выявить уязвимые места панели оператора, через которые злоумышленник может реализовать атаку. Также получилось отобрать 23 уязвимости, касающиеся взаимодействия панели с ПЛК. Из выбранного списка были сформированы 4 варианта атаки злоумышленника на АСУ ТП в целом.

Библиографический список:

1. Опасности, связанные с атаками на АСУ ТП, и методы их эффективной защиты. – URL: <https://infocity.tech/2023/09/opasnosti-svjazannye-s-atakami-na-asu-tp-i-metody-ih-effektivnoj-zaschity/> (дата обращения: 24.12.2023).
2. Сенцова А.Ю., Калининская Я.Э. Обеспечение информационной безопасности АСУ ТП: проблемы и методы защиты// Теоретические и прикладные вопросы реализации проектов в области информационной безопасности. Новосибирск, 2021. С. 23-35. – URL: <https://www.elibrary.ru/item.asp?id=47474020> (дата обращения: 25.12.2023).
3. CVE [Электронный ресурс]. – URL: <https://cve.mitre.org/> (дата обращения: 25.12.2023).

**DEVELOPMENT OF ATTACK SCENARIOS ON THE OPERATOR
PANEL IN THE AUTOMATED CONTROL SYSTEM**

Ustinov S.A., Lazarev T.P.

Scientific supervisor – Novokhrestov A.K.

Tomsk State University of Control Systems and Radioelectronics

Keywords: *Operator panel, automated control system, vulnerabilities, Modbus TCP/IP protocol, CVE database, attack scenarios.*

The study focuses on the security problems of automated process control systems, highlights the danger of attacks aimed at the operator panel. In the course of the work, an analysis of the vulnerable component and possible vulnerabilities was carried out. Attack scenarios have also been proposed in which the vulnerability of the Modbus TCP/IP protocol was exploited.