



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кіберзахист об'єктів критичної інфраструктури

Лабораторний практикум №2

Оцінювання вразливостей об'єкту критичної інфраструктури **на основі показника CVSS**

Перевірив:

Войцеховський А. В.

Виконав:

студент I курсу

групи ФБ-41мп

Сахній Н. Р.

Київ 2024

Мета роботи: Ознайомитись із моделлю загроз, типовою для об'єктів критичної інфраструктури на прикладі промислового інтернету речей. Опанувати методику розрахунку показника CVSS на основі Common Vulnerability Scoring System Version 3.1 на прикладі загроз об'єкта критичної інфраструктури.

Завдання до виконання:

1. Зібрати дані про типові для об'єктів інфраструктури відкритого ключа атаки, проаналізувати можливі шляхи здійснення (згідно варіанту).

Варіант №5. Атаки на вразливі протоколи IoT з метою використання даних зв'язку IoT (контроль над сесіями зв'язку, сніффінг інформації тощо) – на прикладі Modbus.

Типові атаки та можливі шляхи здійснення разом з описом

❖ **Атака на незашифровані дані**

Опис: Протокол Modbus передає дані у відкритому вигляді без шифрування, що робить його вразливим до потенційного сніффінгу.

Шлях здійснення: Зловмисник може підключитися до мережі і в пасивному режимі перехоплювати пакети Modbus, використовуючи інструменти для аналізу трафіку, наприклад “Wireshark”.

❖ **Man-in-the-Middle (MitM) атака**

Опис: Modbus не підтримує автентифікацію або перевірку цілісності даних, що робить його вразливим до атак типу “людина посередині”.

Шлях здійснення: Зловмисник може вставити себе між PLC і контролером, перехоплювати, змінювати або перенаправляти команди, таким чином

отримуючи контроль над системою. Це можна зробити через доступ до фізичних мереж або через компрометацію мережевих пристроїв.

❖ Атака Replay (повторення даних)

Опис: Зловмисник може повторно відправити легітимні пакети Modbus, перехоплені раніше, щоб відтворити або змінити попередні дії.

Шлях здійснення: Зловмисник спочатку сніффить законні пакети, що містять команди управління обладнанням. Після чого повторно відправляє ці пакети, щоб викликати ті ж дії на обладнанні. Для таких атак можуть використовуватися інструменти на зразок “tcpreplay”.

❖ Атака на зміну стану обладнання

Опис: Зловмисник може відправляти підроблені запити або команди на зміну стану обладнання. Оскільки Modbus не вимагає перевірки автентичності команд, то це може дозволити змінювати операційні режими обладнання або навіть пошкоджувати його.

Шлях здійснення: Через сніффінг або прямий доступ до мережі можна відправити підроблені команди на зупинку, зміну стану або перевантаження обладнання, що підключено до мережі через Modbus.

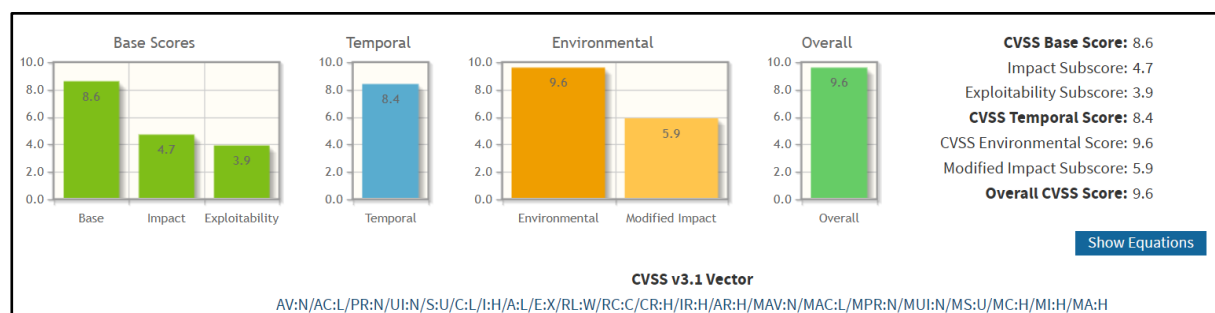
Дослідження відомої вразливості, яка пов’язана із Modbus

Проведемо оцінювання на основі показника CVSS v3.1 проблеми обходу автентифікації за допомогою Capture-Replay, яка була виявлена у протоколі Schneider Electric Modicon Modbus організацією CERT-US весною 2017 р.

Отже, з особистого досвіду та з використанням наукових джерел запишемо ті значення, які можуть приймати метрики досліджуваної вразливості.

Група метрики	Назва метрики та кодове позначення	Фактичне значення	Обов'язкове ?
Base	Attack Vector (AV)	Network (AV:N)	Yes
	Attack Complexity (AC)	Low (AC:L)	Yes
	Privileges Required (PR)	Low (PR:L)	Yes
	User Interaction (UI)	None (UI:N)	Yes
	Scope (S)	Unchanged (S:U)	Yes
	Confidentiality (C)	Low (C:L)	Yes
	Integrity (I)	High (I:H)	Yes
	Availability (A)	High (A:H)	Yes
Temporal	Exploit Code Maturity (E)	Not Defined (E:X)	No
	Remediation Level (RL)	Workaround (RL:W)	No
	Report Confidence (RC)	Confirmed (RC:C)	No
Environmental	Confidentiality Requirement (CR)	High (CR:H)	No
	Integrity Requirement (IR)	High (IR:H)	No
	Availability Requirement (AR)	High (AR:H)	No
	Modified Attack Vector (MAV)	Network (MAV:N)	No
	Modified Attack Complexity (MAC)	Low (MAC:L)	No
	Modified Privileges Required (MPR)	None (MPR:N)	No
	Modified User Interaction (MUI)	None (MUI:N)	No
	Modified Scope (MS)	Unchanged (MS:U)	No
	Modified Confidentiality (MC)	High (MC:H)	No
	Modified Integrity (MI)	High (MI:H)	No
	Modified Availability (MA)	High (MA:H)	No

2. Застосувати [калькулятор фреймворку](#), щоб обчислити CVSS-показники:



3. Зробити висновки про рівень небезпечності для заданого об'єкту КІ.

Загалом атака на протокол Modbus може бути дуже небезпечною для об'єктів КІ через здатність зловмисників безпосередньо впливати на критичні процеси і обладнання, тим самим викликаючи зупинку роботи, а також навіть пошкодження автоматизованих систем управління.

Отже, зважаючи на критичний рівень небезпеки (“Environmental Score”: “9.6 Critical”), який було отримано для заданого об'єкту КІ, можна зробити висновок, що дана вразливість повинна бути негайно усунена. Крім того, високий рівень небезпеки (“Base Score”: “8.6 High”) свідчить про те, що інші організації, які використовують протокол Modbus, також повинні забезпечити належний захист для своєї інфраструктури.

Додатково варто звернути уваги, що CVSS-показник був оцінений досить точно, адже ця відома вразливість ([CVE-2017-6034](#)) має критичний рівень небезпеки (“Base Score”: “9.8 Critical”) за оцінкою професійних експертів:

CVE-2017-6034 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description


An Authentication Bypass by Capture-Replay issue was discovered in Schneider Electric Modicon Modbus Protocol. Sensitive information is transmitted in cleartext in the Modicon Modbus protocol, which may allow an attacker to replay the following commands: run, stop, upload, and download.

Metrics

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

 **NIST: NVD** **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

4. Надати рекомендації по усуненню проблеми на об'єкті КІ.

Рекомендовано вжити захисних заходів, щоб мінімізувати потенційний ризик використання згаданої вище вразливості. Отже, зокрема необхідно:

- Звести до мінімуму доступ до мережі для всіх пристроїв і/або систем керування та переконатися, що вони недоступні з інтернету.
- Розташувати мережі системи керування та віддалені пристрої за брандмауерами та ізолювати їх від бізнес-мережі.
- Якщо потрібен віддалений доступ, використовувати безпечні методи, такі як віртуальні приватні мережі (VPN), усвідомлюючи, що VPN можуть мати вразливі місця та їх слід оновлювати до стабільної версії.

5. Відповісти на контрольні запитання.

▪ Які покращення внесені в CVSS 3.0 порівняно з CVSS 3.1?

Основна зміна у CVSS 3.1 стосується покращення чіткості визначень та інструкцій щодо використання метрик, зокрема щодо метрик Score і розширення Attack Vector. Також зроблено окремий акцент на тому, що CVSS призначений для вимірювання рівня небезпечності вразливості, тож не повинен використовуватися окремо для процесу оцінки ризику.

▪ Які види атак є найбільш небезпечними для об'єктів КІ?

Найбільш небезпечними для об'єктів критичної інфраструктури (КІ) є атаки на мережеві протоколи, зокрема Man-in-the-Middle (MitM), DDoS-атаки, несанкціоновані спроби доступу до даних, а також цільові атаки на системи управління технологічними процесами (SCADA, ICS).

▪ Які підходи до визначення критичності пропонує CVSS?

CVSS пропонує наступних три групи метрик для оцінки рівня безпеки:

- * **Base Score:** оцінює базові властивості незалежно від середовища.

- * **Temporal Score:** враховує зміни, які можуть відбуватися із часом, такі як наявність експлоїтів, виправлень та підтверджень.
- * **Environmental Score:** враховує специфічні умови середовища, де вразливість застосовується, дозволяючи організаціям адаптувати оцінку до своїх умов.

▪ **Які загальні принципи використання концепція [Industry 4.0](#)?**

Концепція Industry 4.0 заснована на інтеграції кібер-фізичних систем, інтернету речей (IoT), хмарних технологій та штучного інтелекту для створення інтелектуальних виробничих процесів, що автоматизують та оптимізують управління виробництвом. Основні принципи включають взаємосумісність, віртуалізацію інформації, можливість роботи в реальному часі та децентралізоване прийняття рішень.