6th Oct 2024

CSCE 5580 : Computer Networks | Project 1: Network Monitoring Tools
Instructor: Tao Wang

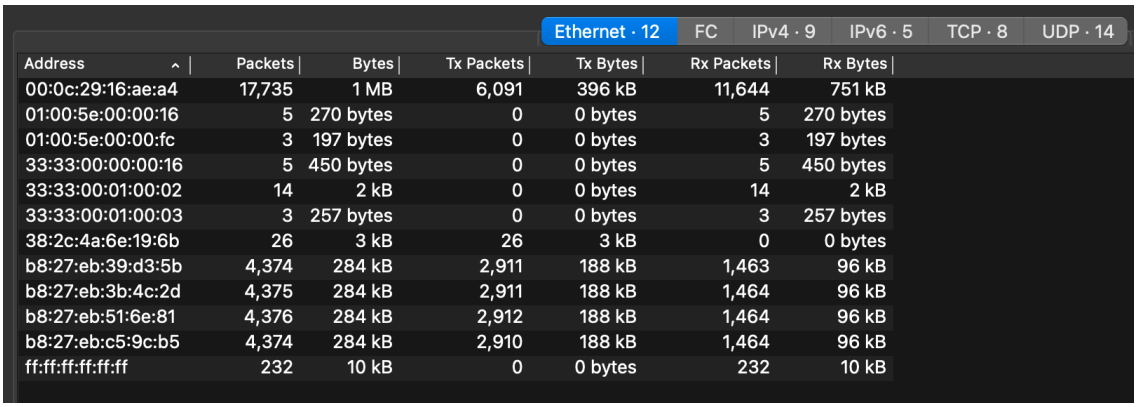
Uday Bhaskar Valapadasu
11696364

Task (1) Solution:

- Wiretapping on the Industrial Control System (**ICS**) network traffic Packet Capture using Wireshark V4.4.0
- The default Modbus port number is **502.**

a) How many unique MAC addresses were on the network?

In total, they are **12** MAC Addresses.



Ethernet · 12 | FC | IPv4 · 9 | IPv6 · 5 | TCP · 8 | UDP · 14

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:0c:29:16:ae:a4	17,735	1 MB	6,091	396 kB	11,644	751 kB
01:00:5e:00:00:16	5	270 bytes	0	0 bytes	5	270 bytes
01:00:5e:00:00:fc	3	197 bytes	0	0 bytes	3	197 bytes
33:33:00:00:00:16	5	450 bytes	0	0 bytes	5	450 bytes
33:33:00:01:00:02	14	2 kB	0	0 bytes	14	2 kB
33:33:00:01:00:03	3	257 bytes	0	0 bytes	3	257 bytes
38:2c:4a:6e:19:6b	26	3 kB	26	3 kB	0	0 bytes
b8:27:eb:39:d3:5b	4,374	284 kB	2,911	188 kB	1,463	96 kB
b8:27:eb:3b:4c:2d	4,375	284 kB	2,911	188 kB	1,464	96 kB
b8:27:eb:51:6e:81	4,376	284 kB	2,912	188 kB	1,464	96 kB
b8:27:eb:c5:9c:b5	4,374	284 kB	2,910	188 kB	1,464	96 kB
ff:ff:ff:ff:ff:ff	232	10 kB	0	0 bytes	232	10 kB

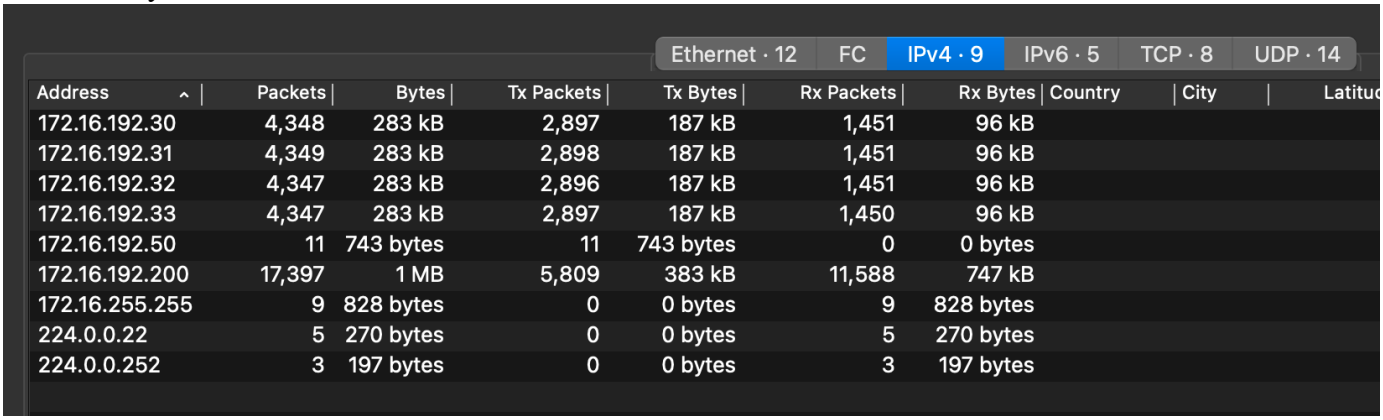
Steps used to find the Mac Address:

1. Open Wireshark and load your PCAP file.
2. Go to **Statistics** > **Endpoints** > Choose **Ethernet Addresses** from the drop menu, adjacent to the search bar under the **Hosts** Tab.

b) How many unique IP addresses were on the network (IPv4 and IPv6)?

1. Open Wireshark and load your PCAP file.
2. Go to **Statistics** > **Endpoints**.
3. Select the **IPv4** tab, we can find the unique IPv4 addresses.

In total, they are **9** IPv4 Addresses



Ethernet · 12 | FC | IPv4 · 9 | IPv6 · 5 | TCP · 8 | UDP · 14

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitu
172.16.192.30	4,348	283 kB	2,897	187 kB	1,451	96 kB			
172.16.192.31	4,349	283 kB	2,898	187 kB	1,451	96 kB			
172.16.192.32	4,347	283 kB	2,896	187 kB	1,451	96 kB			
172.16.192.33	4,347	283 kB	2,897	187 kB	1,450	96 kB			
172.16.192.50	11	743 bytes	11	743 bytes	0	0 bytes			
172.16.192.200	17,397	1 MB	5,809	383 kB	11,588	747 kB			
172.16.255.255	9	828 bytes	0	0 bytes	9	828 bytes			
224.0.0.22	5	270 bytes	0	0 bytes	5	270 bytes			
224.0.0.252	3	197 bytes	0	0 bytes	3	197 bytes			

1. Open Wireshark and load your PCAP file.
2. Go to **Statistics** > **Endpoints**.
3. Select the **IPv6** tab, we can find the unique IPv6 addresses.

In total, they are **5** IPv6 Addresses

Ethernet · 12 | FC | IPv4 · 9 | IPv6 · 5 | TCP · 8 | UDP · 14

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City
fe80::6090:beb3:9385:1c79	7	1 kB	7	1 kB	0	0 bytes		
fe80::bdb7:226e:14ef:5c24	15	2 kB	15	2 kB	0	0 bytes		
ff02::16	5	450 bytes	0	0 bytes	5	450 bytes		
ff02::1:2	14	2 kB	0	0 bytes	14	2 kB		
ff02::1:3	3	257 bytes	0	0 bytes	3	257 bytes		

c) What were the two UDP protocols used?

1. Open Wireshark and load your PCAP file.
2. Go to **Statistics** > **Protocol Hierarchy**.
3. In the drop-down list we can find the **UDP protocols** under **IPv6**.

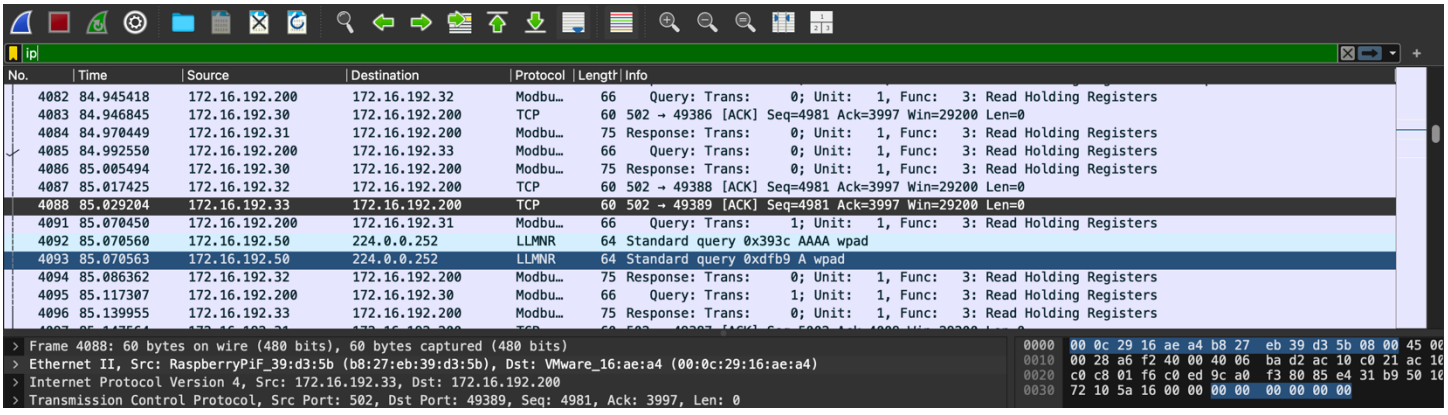
Two UDP protocols are **Link-local Multicast Name Resolution** & **DHCPv6**

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	17761	100.0	1149412	25 k	0	0	0	17761
Ethernet	100.0	17761	24.7	284414	6251	0	0	0	17761
Internet Protocol Version 6	0.1	22	0.1	920	20	0	0	0	22
User Datagram Protocol	0.1	17	0.0	136	2	0	0	0	17
Link-local Multicast Name Resolution	0.0	3	0.0	71	1	3	71	1	3
DHCPv6	0.1	14	0.1	1288	28	14	1288	28	14
Internet Control Message Protocol v6	0.0	5	0.0	140	3	5	140	3	5
Internet Protocol Version 4	98.0	17408	30.3	348180	7653	0	0	0	17408
User Datagram Protocol	0.1	12	0.0	96	2	0	0	0	12
NetBIOS Name Service	0.1	9	0.0	450	9	9	450	9	9
Link-local Multicast Name Resolution	0.0	3	0.0	71	1	3	71	1	3
Transmission Control Protocol	97.9	17391	30.3	347884	7646	5804	116144	2552	17391
Modbus/TCP	65.2	11587	13.6	156414	3438	0	0	0	11587
Modbus	65.2	11587	6.6	75305	1655	11587	75305	1655	11587
Internet Group Management Protocol	0.0	5	0.0	80	1	5	80	1	5
Address Resolution Protocol	1.9	331	0.8	9268	203	331	9268	203	331

d) Which Ethernet address was shared between an IPv4 and IPv6 address?

Step 1: Open Wireshark and load your PCAP file.

Step 2: Search the **Ethernet address** of **IPv4** using the search filter "**ip**".



Step 3: Go to **Statistics** > **Endpoints**.

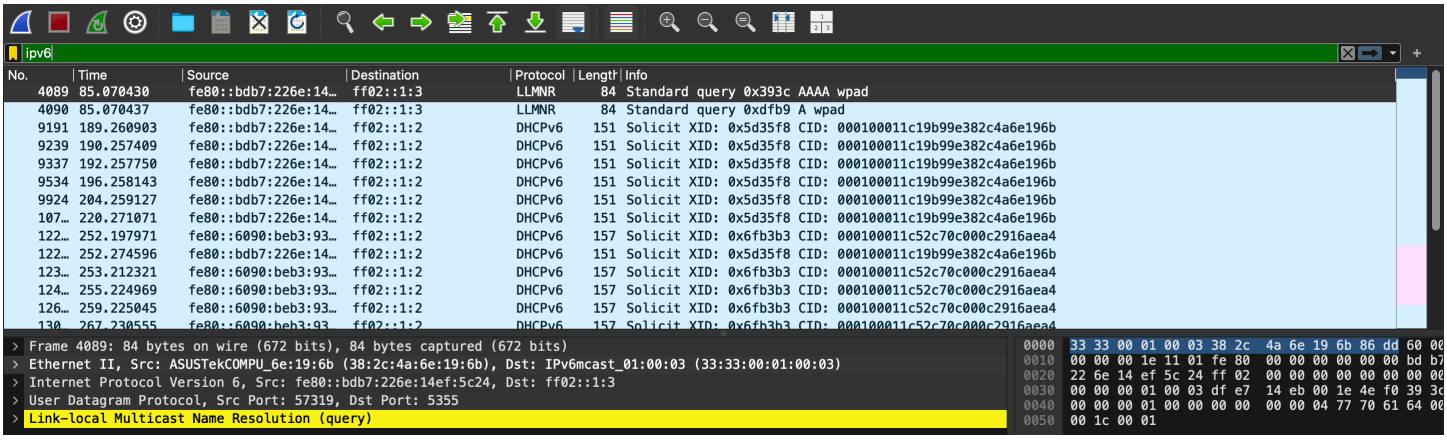
Ethernet · 9 | IPv4 · 9 | IPv6 | TCP · 8 | UDP · 7

Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:0c:29:16:ae:a4	17,397	1 MB	17,735	98.09%	5,809	383 kB	11,588	747 kB
01:00:5e:00:00:16	5	270 bytes	5	100.00%	0	0 bytes	5	270 bytes
01:00:5e:00:00:fc	3	197 bytes	3	100.00%	0	0 bytes	3	197 bytes
38:2c:4a:6e:19:6b	11	743 bytes	26	42.31%	11	743 bytes	0	0 bytes
b8:27:eb:39:d3:5b	4,347	283 kB	4,374	99.38%	2,897	187 kB	1,450	96 kB
b8:27:eb:3b:4c:2d	4,348	283 kB	4,375	99.38%	2,897	187 kB	1,451	96 kB
b8:27:eb:51:6e:81	4,349	283 kB	4,376	99.38%	2,898	187 kB	1,451	96 kB
b8:27:eb:c5:9c:b5	4,347	283 kB	4,374	99.38%	2,896	187 kB	1,451	96 kB
ff:ff:ff:ff:ff:ff	9	828 bytes	232	3.88%	0	0 bytes	9	828 bytes

- They are total of 9 Ethernet addresses associated with IPv4
- Note down all mac addresses in Excel Sheet.

IPv4 - Ethernet Address
00:0c:29:16:ae:a4
01:00:5e:00:00:16
01:00:5e:00:00:fc
38:2c:4a:6e:19:6b
b8:27:eb:39:d3:5b
b8:27:eb:3b:4c:2d
b8:27:eb:51:6e:81
b8:27:eb:c5:9c:b5

Step 4: Similarily Searching the **Ethernet address** of **IPv6** using the search filter "**ipv6**".



Step 5: Go to **Statistics** > **Endpoints**.

Ethernet · 5 | IPv4 | IPv6 · 5 | TCP | UDP · 7

Address	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:0c:29:16:ae:a4	7	1 kB	17,735	0.04%	7	1 kB	0	0 bytes
33:33:00:00:00:16	5	450 bytes	5	100.00%	0	0 bytes	5	450 bytes
33:33:00:01:00:02	14	2 kB	14	100.00%	0	0 bytes	14	2 kB
33:33:00:01:00:03	3	257 bytes	3	100.00%	0	0 bytes	3	257 bytes
38:2c:4a:6e:19:6b	15	2 kB	26	57.69%	15	2 kB	0	0 bytes

- They are total of 5 Ethernet addresses associated with IPv6.
- Note down all mac addresses in Excel Sheet

IPv4 - Ethernet Address	IPv6 - Ethernet Address
00:0c:29:16:ae:a4	00:0c:29:16:ae:a4
01:00:5e:00:00:16	33:33:00:00:00:16
01:00:5e:00:00:fc	33:33:00:01:00:02
38:2c:4a:6e:19:6b	33:33:00:01:00:03
b8:27:eb:39:d3:5b	38:2c:4a:6e:19:6b
b8:27:eb:3b:4c:2d	
b8:27:eb:51:6e:81	
b8:27:eb:c5:9c:b5	

Step 6: Compare the the IPv4 & IPv6 Ethernet address and find the common Ethernet addresses(Mac Addressses)

IPv4 - Ethernet Address	IPv6 - Ethernet Address
00:0c:29:16:ae:a4	00:0c:29:16:ae:a4
01:00:5e:00:00:16	33:33:00:00:00:16
01:00:5e:00:00:fc	33:33:00:01:00:02
38:2c:4a:6e:19:6b	33:33:00:01:00:03
b8:27:eb:39:d3:5b	38:2c:4a:6e:19:6b
b8:27:eb:3b:4c:2d	
b8:27:eb:51:6e:81	
b8:27:eb:c5:9c:b5	

The Ethernet address shared between both IPv4 and IPv6 traffic is:

- **00:0c:29:16:ae:a4**
- **38:2c:4a:6e:19:6b**

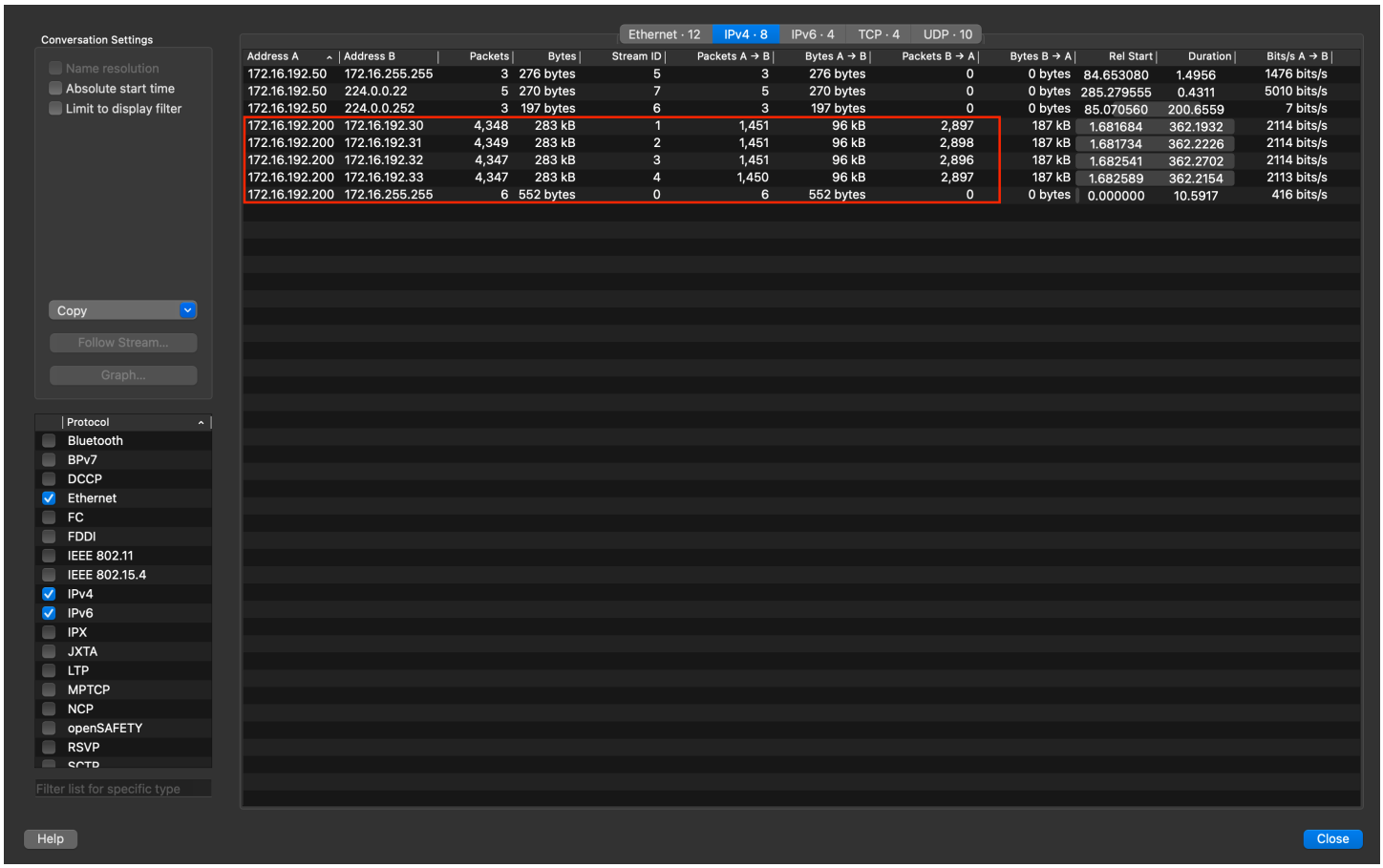
e) It seems that there is a Human-Machine Interface (HMI) server that interacts with multiple devices in the network through Modbus. What is the IP address of the server?

- **Opened Wireshark** and loaded the network capture file (PCAP).
- **Navigated to Statistics**:
  - I went to **Statistics > Conversations** to display communication between devices.
- **Analyzed IPv4 Conversations**:
  - I checked the **IPv4 tab** to view IP addresses that communicated frequently.
  - I looked for the IP address that interacted with **multiple devices** and exchanged a large number of packets.
- **Identified the HMI Server**:
  - I determined that the IP address with the most conversations and high packet counts was likely the **HMI server**.

HMI Server IP Address : - **172.16.192.200**

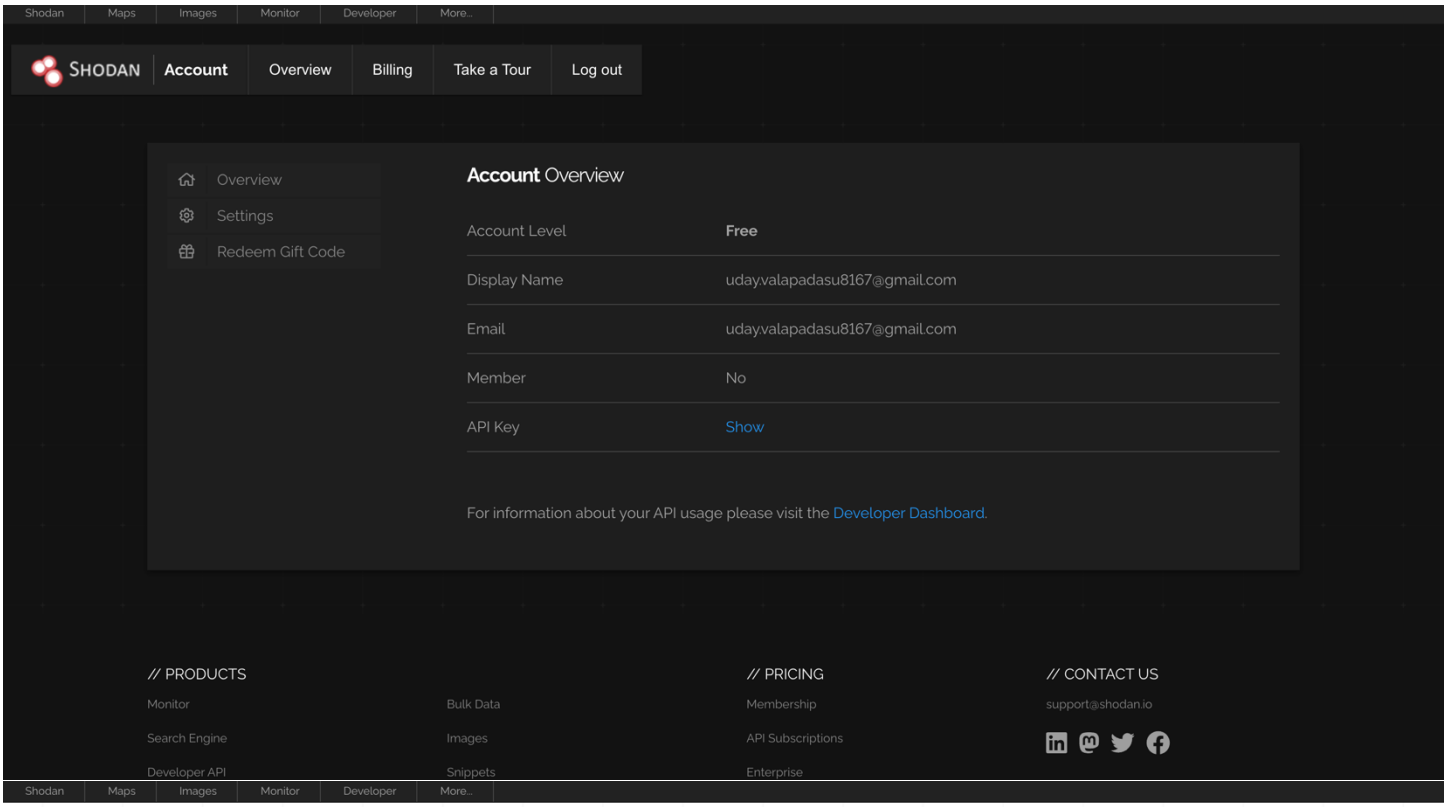
- I observed that the IP address **172.16.192.200** was consistently communicating with multiple devices, specifically 172.16.192.30, 172.16.192.31, 172.16.192.32, and 172.16.192.33.

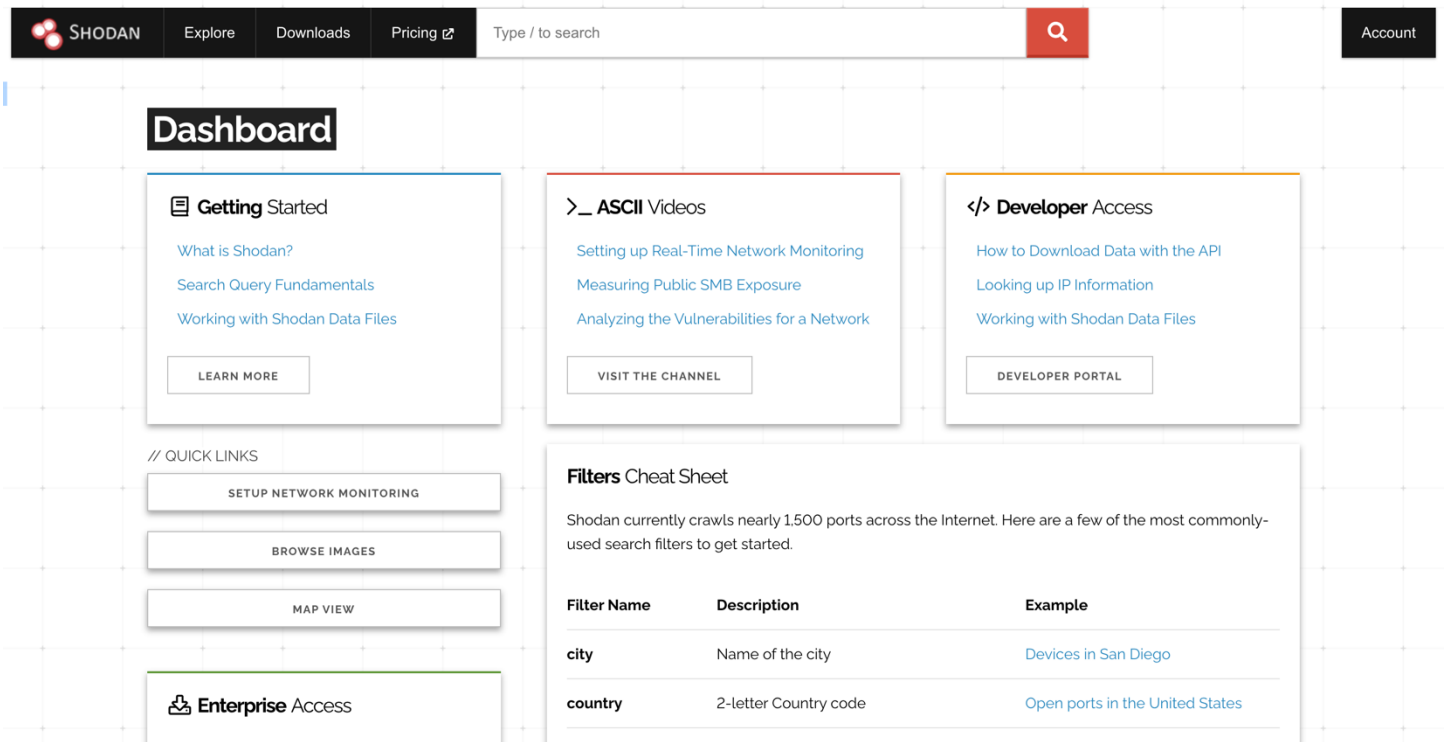
- Each of these interactions involved a **high number of packets**, approximately 4,348 packets, indicating frequent communication. This level of activity is typical for a Human-Machine Interface (HMI) server that manages communication with various devices on the network.



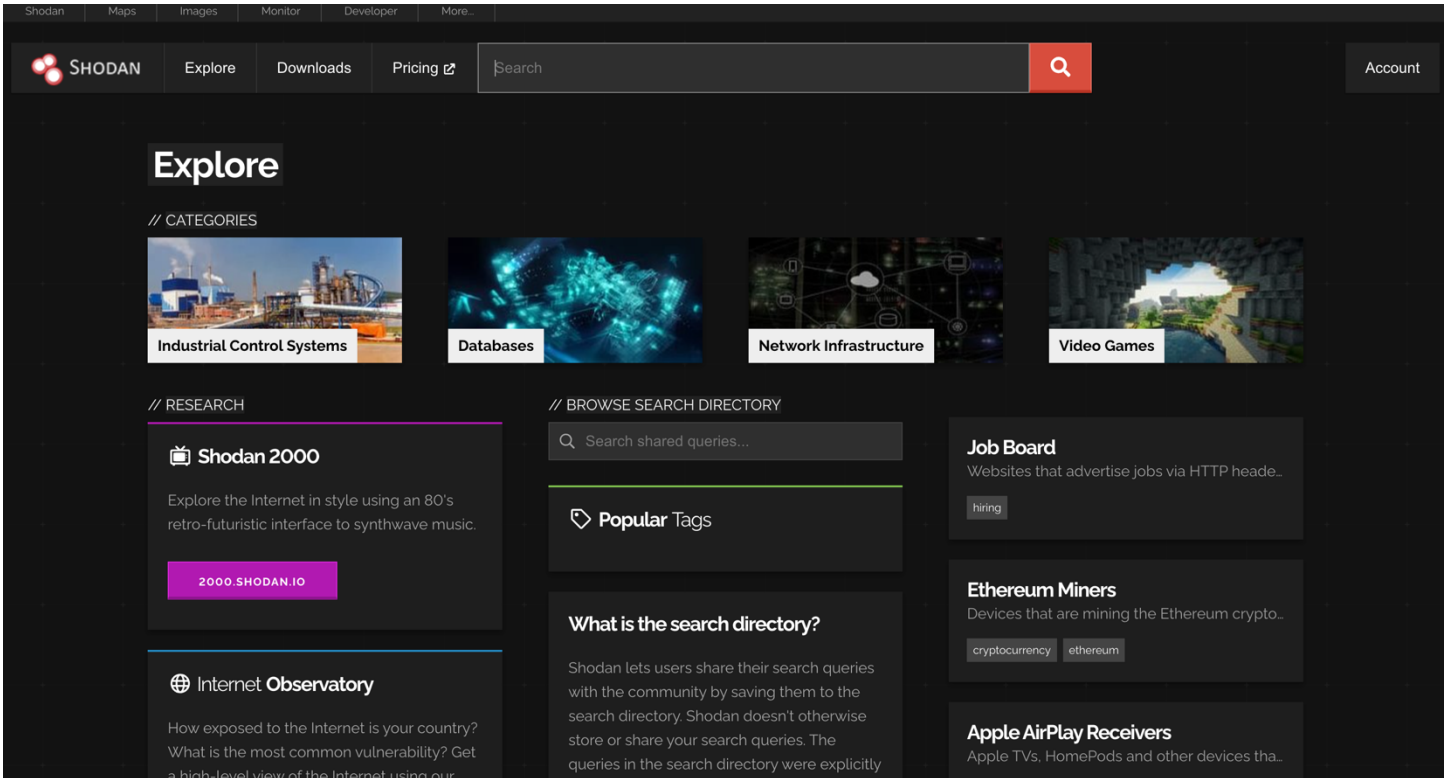
Task (2) Solution:

Step 1: Registered onto www.shodan.io

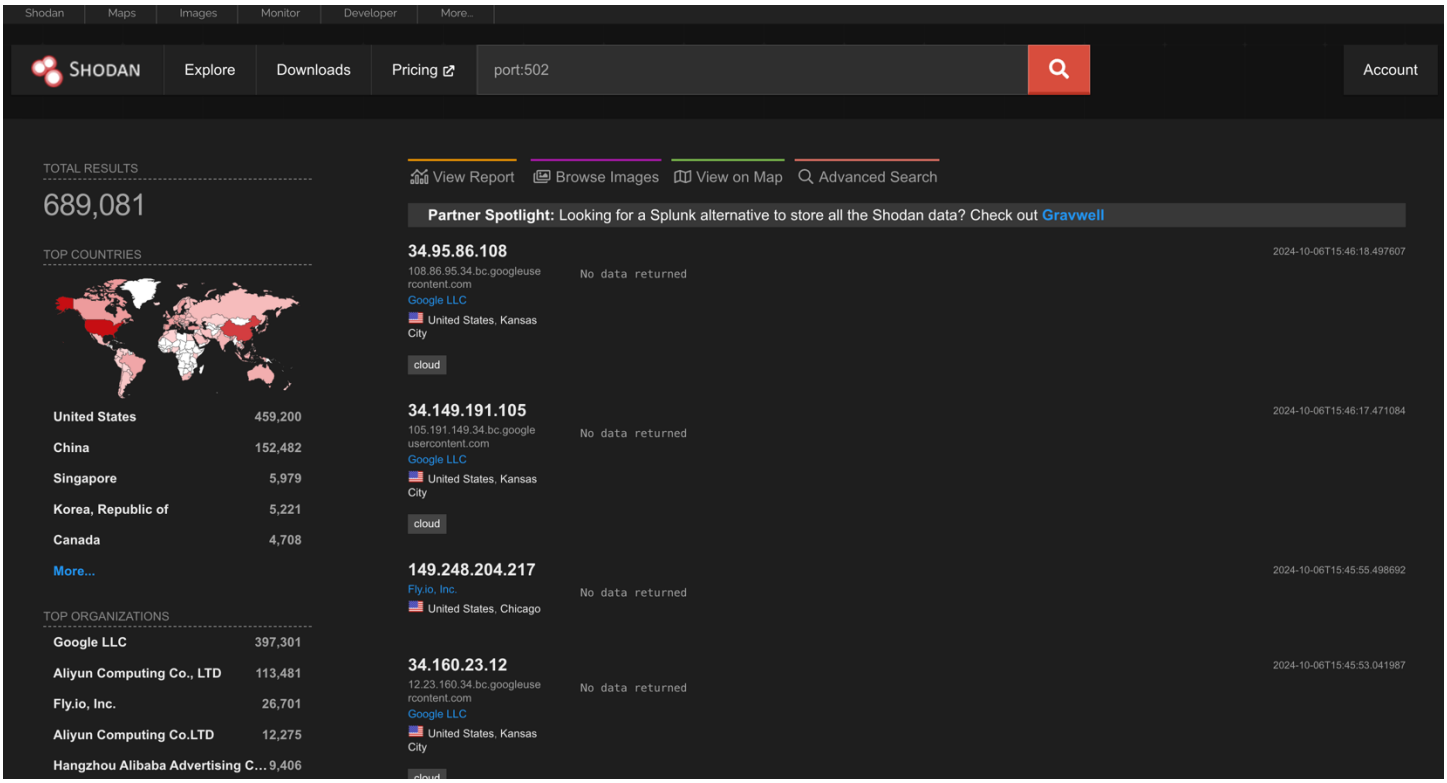




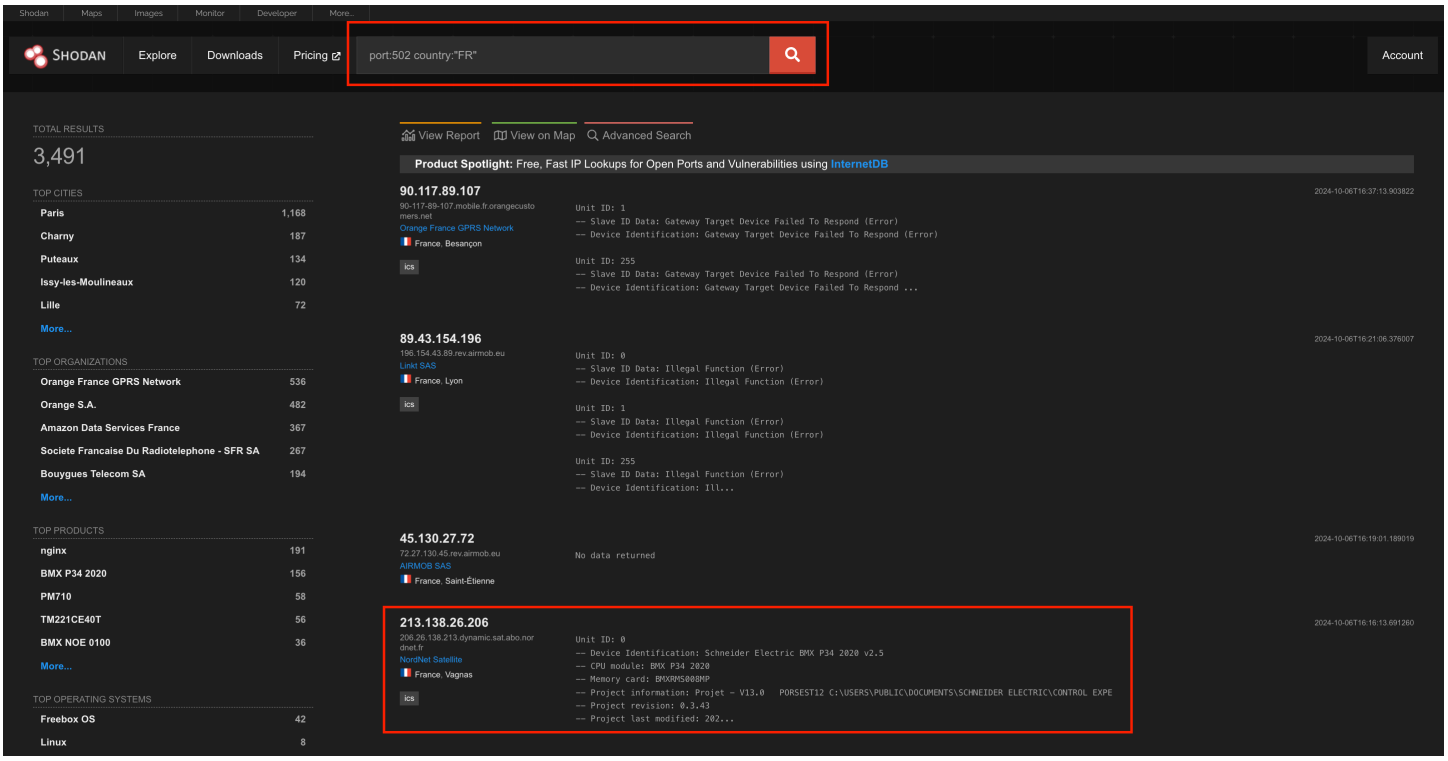
Step 2: Click on **explore tab** at the top.



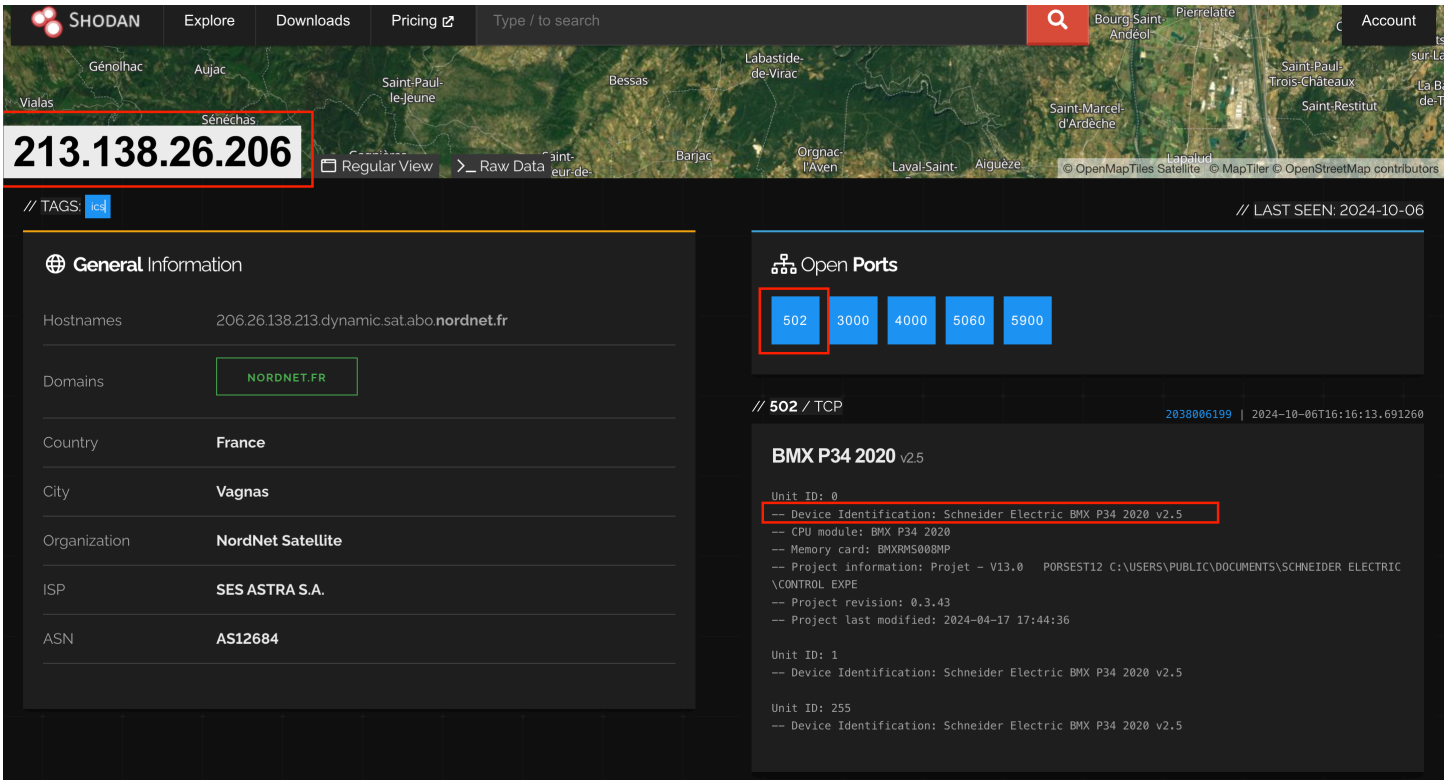
Step 3: Search for "**port:502**" at the top.



Step 4: Once the results appeared, I have choosen “**France**” country to explore. Found **one device**/IP address returned by shodan that does not show “**error**” or **illegal device type.**



Step 6: Analysis the **Summary** of the Device. Searched the 502 port Information & Device Type: “**Schneider Electric BMX P34 2020 v2.5 ”**.



Step 7: Found the device **vulnerabilities** associated with the device on Google.

URL: https://www.cisa.gov/news-events/ics-advisories/icsa-20-016-01

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / ICS Advisory

SHARE:

ICS ADVISORY

Schneider Electric Modicon Controllers (Update A)

Last Revised: April 03, 2020 **Alert Code:** ICSA-20-016-01

1. EXECUTIVE SUMMARY

- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Schneider Electric
- **Equipment:** Modicon M580, Modicon M340, Modicon Quantum, and Modicon Premium
- **Vulnerability:** Improper Check for Unusual or Exceptional Conditions

2. UPDATE INFORMATION

This updated advisory is a follow-up to the original advisory titled ICSA-20-016-01 Schneider Electric Modicon Controllers that was published January 16, 2020, on the ICS webpage on us-cert.gov

4.2 VULNERABILITY OVERVIEW

4.2.1 IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS CWE-754

This vulnerability could cause a denial-of-service condition in the controller when reading specific memory blocks using Modbus TCP.

CVE-2019-6857 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

4.2.2 IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS CWE-754

This vulnerability could cause a denial-of-service condition when writing specific physical memory blocks using Modbus TCP.

CVE-2019-6856 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

4.2.3 IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS CWE-754

This vulnerability could cause a denial-of-service condition when reading data with invalid index using Modbus TCP.

--------- Begin Update A Part 1 of 1 ---------

CVE-2018-7794 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

--------- End Update A Part 1 of 1 ---------

Vulnerability Overview Report:

Several high-severity vulnerabilities have been discovered in Schneider Electric's Modicon series of Programmable Logic Controllers (PLCs), which are extensively deployed in critical infrastructure sectors. This report provides an overview of the key vulnerabilities impacting the Modicon M580, M340, Quantum, and Premium models.

Vulnerabilities Found:

They are three main vulnerabilities that is identified, which are related to improper checks for unusual or exceptional conditions (CWE-754):

1. CVE-2019-6857

- Affects: M580, M340, Premium, and Quantum controllers
- Cause: Improper checks when reading specific memory blocks via Modbus TCP
- Impact: Potential Denial-of-Service (DoS)
- Severity: High (CVSS v3 base score: 7.5)

2. **CVE-2019-6856**

- Affects: M580, M340, Premium, and Quantum controllers
- Cause: Improper checks when writing specific physical memory blocks via Modbus TCP
- Impact: Potential DoS
- Severity: High (CVSS v3 base score: 7.5)

3. **CVE-2018-7794**

- Affects: M580, M340, Premium, and Quantum controllers
- Cause: Reading data with an invalid index using Modbus TCP
- Impact: Potential DoS
- Severity: High (CVSS v3 base score: 7.5)

Risk Assessment

These vulnerabilities are highly concerning because they can be exploited remotely with minimal skill, leading to potential disruptions, safety hazards, and financial losses in critical infrastructure.

Mitigation Strategies

1. Ensure firmware is up to date:
    - Modicon M580: Upgrade to version 3.10
    - Modicon M340: Upgrade to version 3.20
    - Modicon Premium: Upgrade to version 3.20 (contact customer support)
    - Modicon Quantum: Upgrade to version 3.60 (contact customer support)
2. Follow recommended security practices:
- Segregate control networks
- Apply physical access restrictions
- Use secure programming techniques
- Limit internet connectivity
- Employ secure methods for remote access

Conclusion

The found vulnerabilities in Schneider Electric's Modicon controllers pose a substantial risk to critical infrastructure operations. Immediate action, such as firmware updates and adherence to cybersecurity best practices, is required to reduce these risks and assure system security and reliability.