

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:b6		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 Latitude
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.

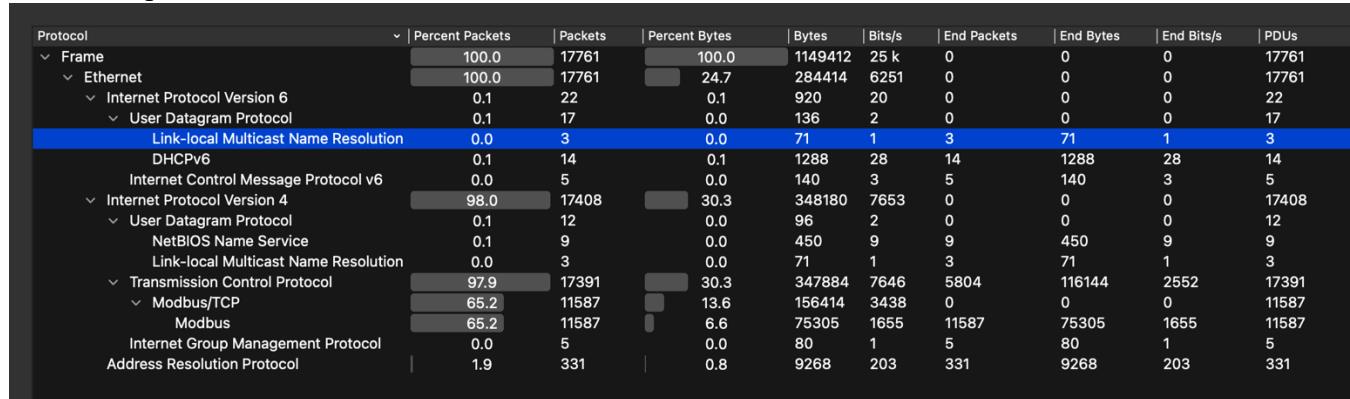
In total, they are **5** IPv6 Addresses

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**.

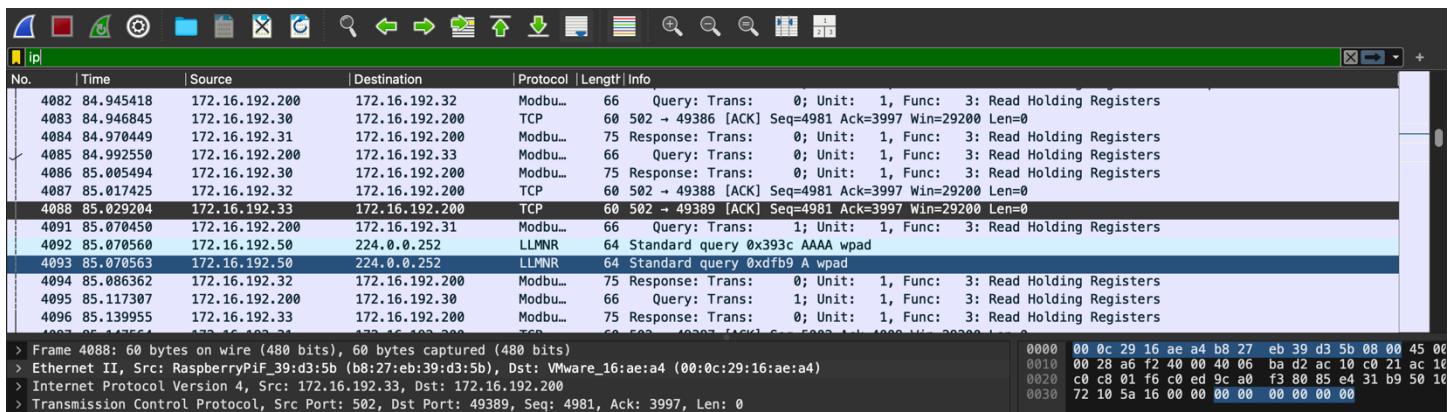
Two UDP protocols are **Link-local Multicast Name Resolution & DHCPv6**



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”.



- 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 Addresses)

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.

Conversation Settings

Address A		Address B		Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
172.16.192.50	172.16.255.255			3	276 bytes	5	3	276 bytes	0	0 bytes	84.653080	1.4956	1476 bits/s
172.16.192.50	224.0.0.22			5	270 bytes	7	5	270 bytes	0	0 bytes	285.279555	0.4311	5010 bits/s
172.16.192.50	224.0.0.252			3	197 bytes	6	3	197 bytes	0	0 bytes	85.070561	200.6559	7 bits/s
172.16.192.200	172.16.192.30			4,348	283 kB	1	1,451	96 kB	2,897	187 kB	1.681684	362.1932	2114 bits/s
172.16.192.200	172.16.192.31			4,349	283 kB	2	1,451	96 kB	2,898	187 kB	1.681734	362.2226	2114 bits/s
172.16.192.200	172.16.192.32			4,347	283 kB	3	1,451	96 kB	2,896	187 kB	1.682541	362.2702	2114 bits/s
172.16.192.200	172.16.192.33			4,347	283 kB	4	1,450	96 kB	2,897	187 kB	1.682589	362.2154	2113 bits/s
172.16.192.200	172.16.255.255			6	552 bytes	0	6	552 bytes	0	0 bytes	0.000000	10.5917	416 bits/s

Copy Follow Stream... Graph...

Protocol:

- Bluetooth
- BPv7
- DCCP
- Ethernet
- FC
- FDDI
- IEEE 802.11
- IEEE 802.15.4
- IPv4
- IPv6
- IPX
- JXTA
- LTP
- MPTCP
- NCP
- openSAFETY
- RSVP
- S-TP

Filter list for specific type

Help Close

Task (2) Solution:

Step 1: Registered onto www.shodan.io

The screenshot shows the Shodan Account Overview page. At the top, there's a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More. Below that is a secondary navigation bar with Account, Overview, Billing, Take a Tour, and Log out. The main content area is titled "Account Overview" and contains the following information:

Setting	Value
Account Level	Free
Display Name	udayvalapadasu8167@gmail.com
Email	udayvalapadasu8167@gmail.com
Member	No
API Key	Show

Below this, a note says: "For information about your API usage please visit the [Developer Dashboard](#)".

The screenshot shows the Shodan homepage. It features three main sections: "PRODUCTS" (Monitor, Search Engine, Developer API), "PRICING" (Membership, API Subscriptions, Enterprise), and "CONTACT US" (support@shodan.io, social media links). At the bottom, there's a navigation bar with Shodan, Maps, Images, Monitor, Developer, and More, followed by a search bar and an "Account" button.

The screenshot shows the Shodan Dashboard. It includes several cards: "Getting Started" (What is Shodan?, Search Query Fundamentals, Working with Shodan Data Files, LEARN MORE), "ASCII Videos" (Setting up Real-Time Network Monitoring, Measuring Public SMB Exposure, Analyzing the Vulnerabilities for a Network, VISIT THE CHANNEL), "Developer Access" (How to Download Data with the API, Looking up IP Information, Working with Shodan Data Files, DEVELOPER PORTAL), and "Filters Cheat Sheet" (a table of common search filters like city, country, and port). There are also quick links for Setup Network Monitoring, Browse Images, and Map View.

Step 2: Click on explore tab at the top.

The screenshot shows the Shodan Explore page. At the top, there are navigation links: Shodan, Maps, Images, Monitor, Developer, More..., Explore, Downloads, Pricing, and Account. A search bar with a magnifying glass icon is centered. Below the search bar, the word "Explore" is displayed in a large, bold font. There are four main categories shown as cards: "Industrial Control Systems" (with an image of a factory), "Databases" (with an image of a network diagram), "Network Infrastructure" (with an image of a network visualization), and "Video Games" (with an image of a video game environment). Under the "RESEARCH" section, there is a card for "Shodan 2000" featuring a retro-futuristic interface and a link to "2000.SHODAN.IO". Another card for "Internet Observatory" shows a map of the world with red dots indicating internet exposure. To the right, under "BROWSE SEARCH DIRECTORY", there is a search bar for "Search shared queries...", a "Popular Tags" section, and a "What is the search directory?" section explaining the purpose of the search directory. Other cards include "Job Board" (listing "hiring"), "Ethereum Miners" (listing "cryptocurrency" and "ethereum"), and "Apple AirPlay Receivers".

Step 3: Search for “port:502” at the top.

The screenshot shows the Shodan search results for "port:502". The search bar at the top contains the query "port:502". The results are displayed in a grid format. The first result is for IP address 34.95.86.108, located in the United States, Kansas City, with a "cloud" tag. The second result is for IP address 34.149.191.105, located in the United States, Kansas City, with a "cloud" tag. The third result is for IP address 149.248.204.217, located in the United States, Chicago, with a "cloud" tag. The results also show the date of the search (2024-10-06T15:46:18.497607) and the number of results (689,081). On the left, there are sections for "TOP COUNTRIES" (United States: 459,200, China: 152,482, Singapore: 5,979, Korea, Republic of: 5,221, Canada: 4,708, More...) and "TOP ORGANIZATIONS" (Google LLC: 397,301, Aliyun Computing Co., LTD: 113,481, Fly.io, Inc.: 26,701, Aliyun Computing Co.LTD: 12,275, Hangzhou Alibaba Advertising C...: 9,406). At the bottom, there are links for "View Report", "Browse Images", "View on Map", and "Advanced Search".

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

The screenshot shows the Shodan search interface with a red box highlighting the search bar containing "port:502 country:'FR'". The results page displays various device details, including IP addresses, unit IDs, and device types. One result is highlighted with a red box, showing an IP address of 213.138.26.206, located in Vagnas, France, with a Schneider Electric BMX P34 2020 v2.5 device type.

Category	Details	Last Seen
TOTAL RESULTS	3,491	
TOP CITIES	Paris (1,168), Charny (187), Puteaux (134), Issy-les-Moulineaux (120), Lille (72)	2024-10-06T16:37:13.903Z
TOP ORGANIZATIONS	Orange France GPRS Network (536), Orange S.A. (482), Amazon Data Services France (367), Societe Francaise Du Radiotéléphone - SFR SA (267), Bouygues Telecom SA (194)	2024-10-06T16:21:06.376Z
TOP PRODUCTS	nginx (191), BMX P34 2020 (156), PM710 (58), TM221CE40T (56), BMX NOE 0100 (36)	2024-10-06T16:19:01.189Z
TOP OPERATING SYSTEMS	Freebox OS (42), Linux (8)	2024-10-06T16:16:13.691Z

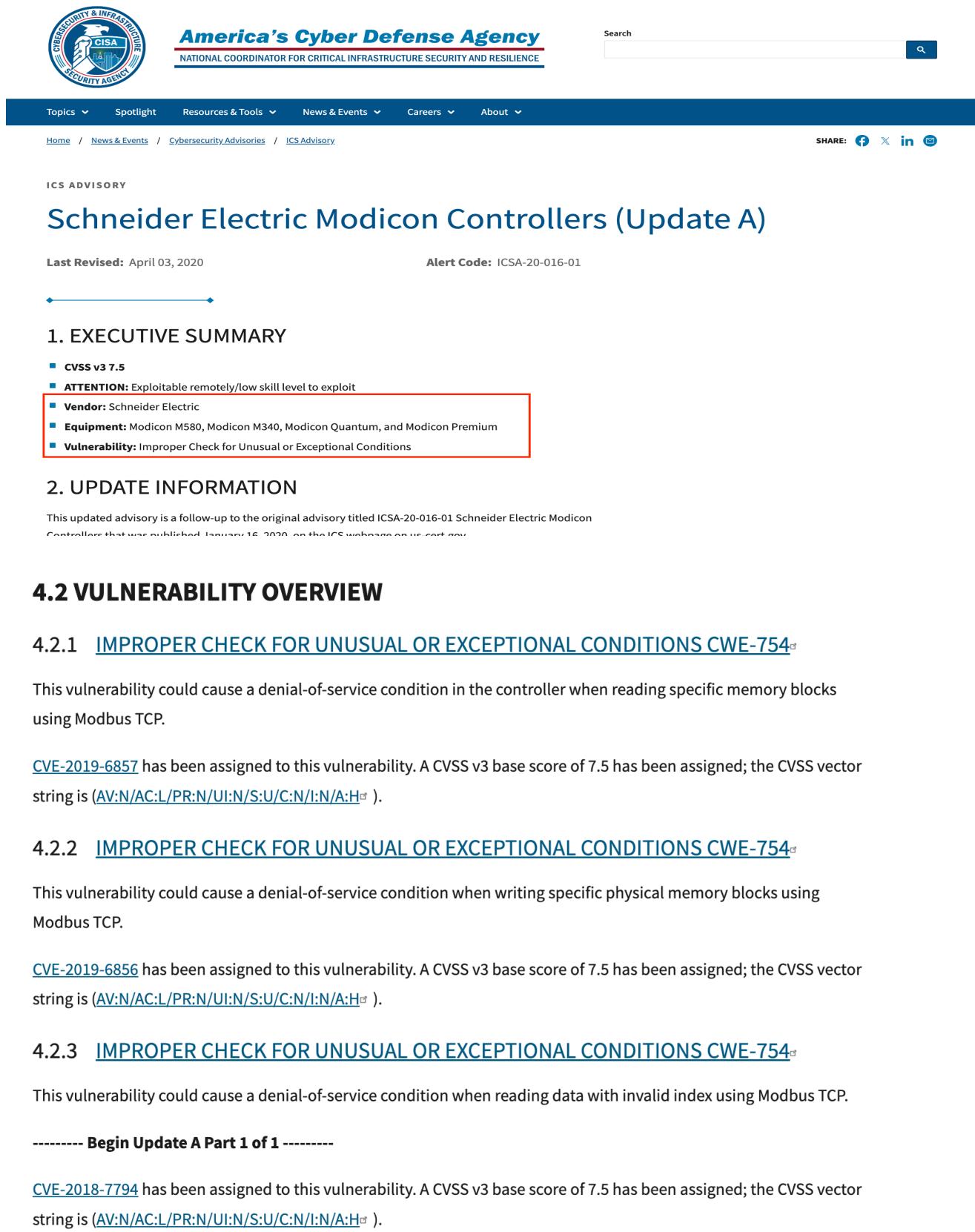
Step 6: Analysis the Summary of the Device. Searched the 502 port Information & Device Type: “Schneider Electric BMX P34 2020 v2.5”.

The screenshot shows the Shodan device summary for IP 213.138.26.206. The device is identified as a Schneider Electric BMX P34 2020 v2.5. The "Open Ports" section highlights port 502, which is also the primary focus of the summary. The "General Information" section provides details about the device's location (Vagnas, France) and network connection (NordNet Satellite).

Category	Details
Hostnames	206.26.138.213.dynamic.sat.abo.nordnet.fr
Domains	NORDNET.FR
Country	France
City	Vagnas
Organization	NordNet Satellite
ISP	SES ASTRA S.A.
ASN	AS12684

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>



The screenshot shows the official website of the U.S. Cybersecurity & Infrastructure Security Agency (CISA). The header features the CISA logo and the text "America's Cyber Defense Agency" and "NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE". A search bar and a navigation menu with links to "Topics", "Spotlight", "Resources & Tools", "News & Events", "Careers", and "About" are visible. Below the header, a breadcrumb trail shows "Home / News & Events / Cybersecurity Advisories / ICS Advisory". On the right, there are social media sharing icons for Facebook, Twitter, LinkedIn, and Email. The main content area is titled "ICS ADVISORY" and "Schneider Electric Modicon Controllers (Update A)". It includes a "Last Revised" date of April 03, 2020, and an "Alert Code" of ICSA-20-016-01. The "1. EXECUTIVE SUMMARY" section contains a bulleted list of details, with the last four items ("Vendor", "Equipment", and "Vulnerability") highlighted by a red rectangular box. The "2. UPDATE INFORMATION" section notes that this is a follow-up to the original advisory ICSA-20-016-01. The "4.2 VULNERABILITY OVERVIEW" section is expanded to show three sub-sections: "4.2.1 IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS CWE-754", "4.2.2 IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS CWE-754", and "4.2.3 IMPROPER CHECK FOR UNUSUAL OR EXCEPTIONAL CONDITIONS CWE-754". Each sub-section describes a denial-of-service condition caused by improper checks for unusual or exceptional conditions during Modbus TCP operations. CVSS scores and vector strings are provided for each vulnerability, along with a reference to the corresponding CVE entry (e.g., CVE-2019-6856).

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^o).

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^o).

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 -----

[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^o).

----- End Update A Part 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:

There are three main vulnerabilities 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.