Fall 2022: ITIS 6167/8167: Network Security

Project 1: Network Security Monitoring Tools

Student Name: Sireesha Ponnaganti

Student email:sponnaga@uncc.edu

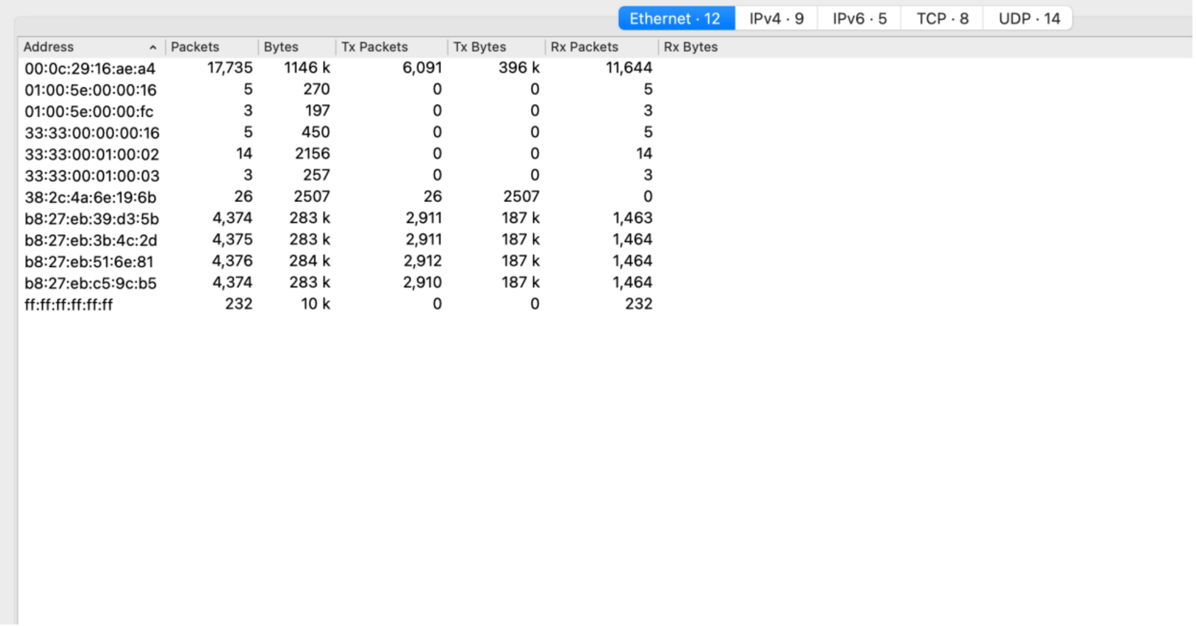
Student ID:801310488

Task (1)

2. Use Wireshark to open the packet capture file that we provide. Please note that the file contains some Industrial Control System (ICS) network traffic that we capture. It uses a protocol called Modbus. You can use google to figure out the protocol and port number that Modbus uses.

In this capture file, please answer the following questions:

a) **How many unique MAC addresses were on the network?**
Answer: The total number of unique MAC addresses on the network are 12. Please refer the figure 2(a).

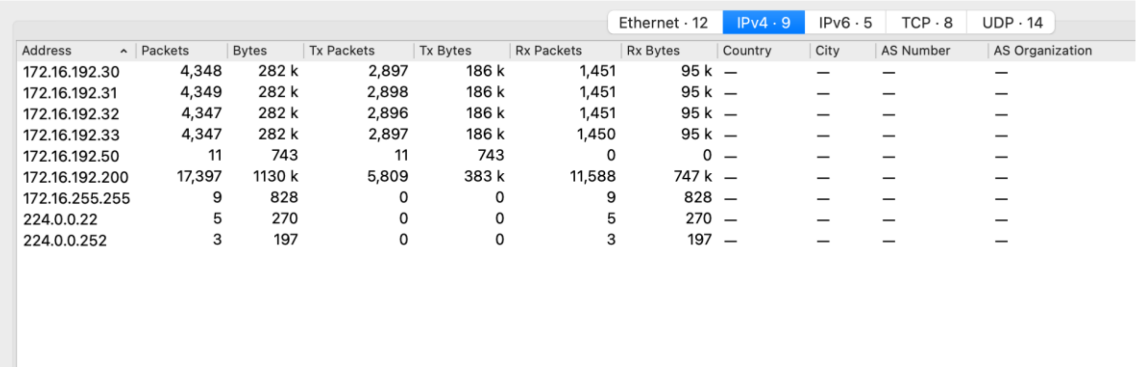


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:0c:29:16:ae:a4	17,735	1146 k	6,091	396 k	11,644	
01:00:5e:00:00:16	5	270	0	0	5	
01:00:5e:00:00:fc	3	197	0	0	3	
33:33:00:00:00:16	5	450	0	0	5	
33:33:00:01:00:02	14	2156	0	0	14	
33:33:00:01:00:03	3	257	0	0	3	
38:2c:4a:6e:19:6b	26	2507	26	2507	0	
b8:27:eb:39:d3:5b	4,374	283 k	2,911	187 k	1,463	
b8:27:eb:3b:4c:2d	4,375	283 k	2,911	187 k	1,464	
b8:27:eb:51:6e:81	4,376	284 k	2,912	187 k	1,464	
b8:27:eb:c5:9c:b5	4,374	283 k	2,910	187 k	1,464	
ff:ff:ff:ff:ff:ff	232	10 k	0	0	232	

Figure 2(a): Total 12 MAC addresses

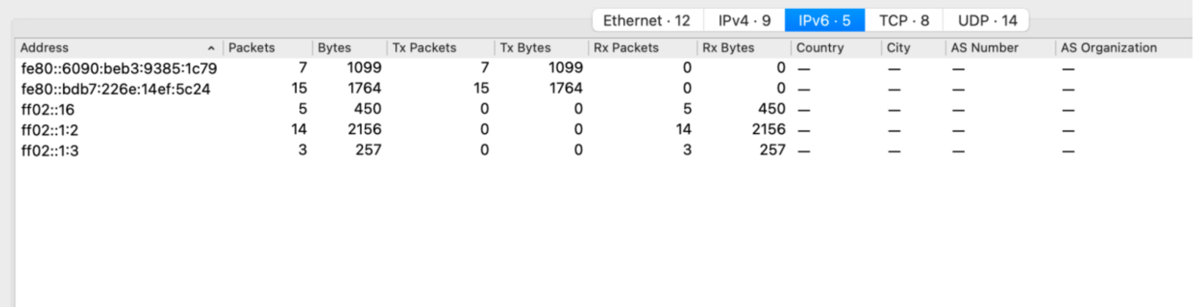
b) How many unique IP addresses were on the network (IPv4 and IPv6)?

Answer: The total number of unique IP addresses on the network of IPV4 were 9 whereas the total number of IPV6 addresses are 5. So, the total number of unique IPV4 and IPV6 addresses are 14. Please refer the figure 2(b1) and figure 2(b2).



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
172.16.192.30	4,348	282 k	2,897	186 k	1,451	95 k	—	—	—	—
172.16.192.31	4,349	282 k	2,898	186 k	1,451	95 k	—	—	—	—
172.16.192.32	4,347	282 k	2,896	186 k	1,451	95 k	—	—	—	—
172.16.192.33	4,347	282 k	2,897	186 k	1,450	95 k	—	—	—	—
172.16.192.50	11	743	11	743	0	0	—	—	—	—
172.16.192.200	17,397	1130 k	5,809	383 k	11,588	747 k	—	—	—	—
172.16.255.255	9	828	0	0	9	828	—	—	—	—
224.0.0.22	5	270	0	0	5	270	—	—	—	—
224.0.0.252	3	197	0	0	3	197	—	—	—	—

Figure 2(b1): Total number of IPV4 addresses are 9



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
fe80::6090:beb3:9385:1c79	7	1099	7	1099	0	0	—	—	—	—
fe80::bdb7:226e:14ef:5c24	15	1764	15	1764	0	0	—	—	—	—
ff02::16	5	450	0	0	5	450	—	—	—	—
ff02::1:2	14	2156	0	0	14	2156	—	—	—	—
ff02::1:3	3	257	0	0	3	257	—	—	—	—

Figure 2(b2): Total number of IPV6 addresses are 5

c) What were the two UDP protocols used?

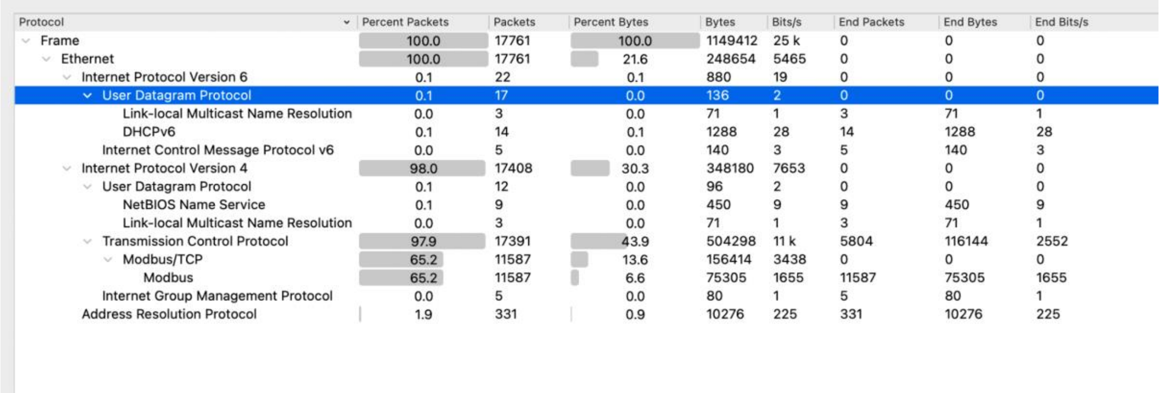
Answer: There are 3 UDP protocols that have been used. They are

1.Link-local Multicast Name Resolution

2.DHCP v6

3. NetBIOS Name Service

Please refer the figure 2(c)



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	17761	100.0	1149412	25 k	0	0	0
Ethernet	100.0	17761	21.6	248654	5465	0	0	0
Internet Protocol Version 6	0.1	22	0.1	880	19	0	0	0
User Datagram Protocol	0.1	17	0.0	136	2	0	0	0
Link-local Multicast Name Resolution	0.0	3	0.0	71	1	3	71	1
DHCPv6	0.1	14	0.1	1288	28	14	1288	28
Internet Control Message Protocol v6	0.0	5	0.0	140	3	5	140	3
Internet Protocol Version 4	98.0	17408	30.3	348180	7653	0	0	0
User Datagram Protocol	0.1	12	0.0	96	2	0	0	0
NetBIOS Name Service	0.1	9	0.0	450	9	9	450	9
Link-local Multicast Name Resolution	0.0	3	0.0	71	1	3	71	1
Transmission Control Protocol	97.9	17391	43.9	504298	11 k	5804	116144	2552
Modbus/TCP	65.2	11587	13.6	156414	3438	0	0	0
Modbus	65.2	11587	6.6	75305	1655	11587	75305	1655
Internet Group Management Protocol	0.0	5	0.0	80	1	5	80	1
Address Resolution Protocol	1.9	331	0.9	10276	225	331	10276	225

Figure 2(c): Illustrates the protocol which have 2 different UDB protocol

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

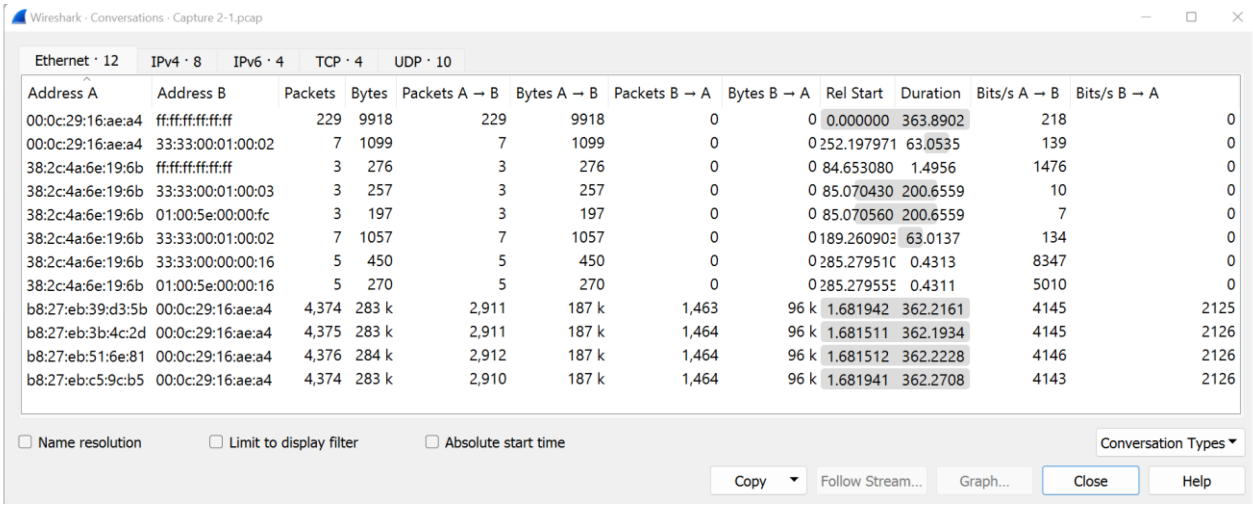
Answer: The Ethernet address that has been shared between the IPV4 and IPV6 address can be fetched with the help of the conversations in the statistics of a Capture file and then applying filter for each and every MAC address which have bidirectional communication. And then, we do take unique IPV4 and IPV6 addresses and check the results for both of them which have common MAC Address.

Upon checking as above method, we found that there are two different MAC addresses that are shared between IPV4 and IPV6 addresses. They are

MAC1=00:0c:29:16:ae:a4, sharing the IPV4 = 172.16.192.200 and IPV6 = fe80::6090:beb3:9385:1c79

MAC2= 38:2c:4a:6e:19:6b, sharing the addresses of IPV4 = 172.16.192.50 and IPV6 = fe80::bdb7:226e:14ef:5c24

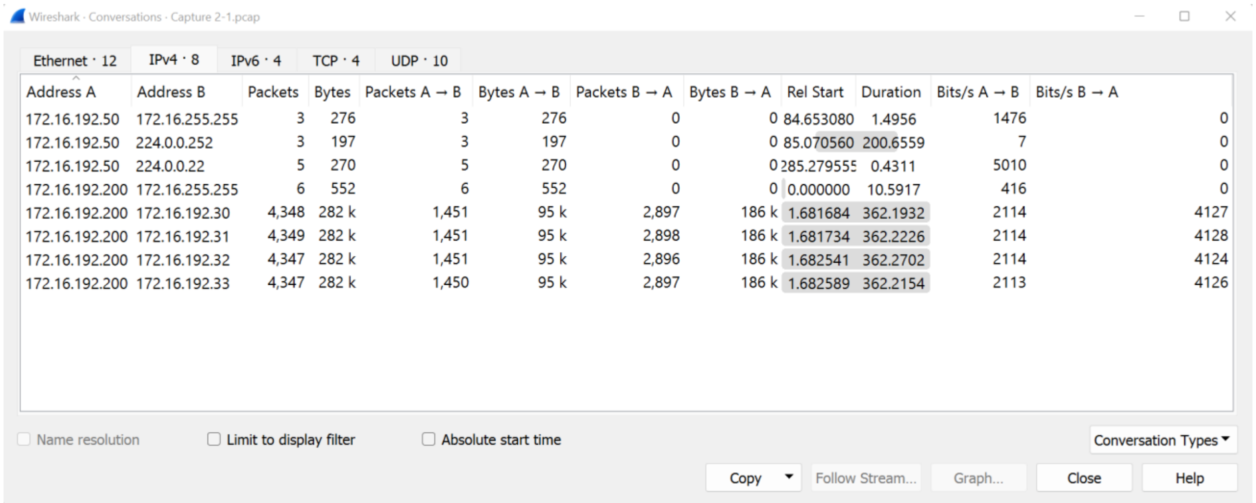
Please refer sample figure(2d1), figure(2d2), figure(2d3) that shows the MAC address that has been shared between IPV4 and IPV6 addresses.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
00:0c:29:16:ae:a4	ff:ff:ff:ff:ff:ff	229	9918	229	9918	0	0	0.000000	363.8902	218	0
00:0c:29:16:ae:a4	33:33:00:01:00:02	7	1099	7	1099	0	0	252.197971	63.0535	139	0
38:2c:4a:6e:19:6b	ff:ff:ff:ff:ff:ff	3	276	3	276	0	0	84.653080	1.4956	1476	0
38:2c:4a:6e:19:6b	33:33:00:01:00:03	3	257	3	257	0	0	85.070430	200.6559	10	0
38:2c:4a:6e:19:6b	01:00:5e:00:00:fc	3	197	3	197	0	0	85.070560	200.6559	7	0
38:2c:4a:6e:19:6b	33:33:00:01:00:02	7	1057	7	1057	0	0	189.26090	63.0137	134	0
38:2c:4a:6e:19:6b	33:33:00:00:00:16	5	450	5	450	0	0	285.27951	0.4313	8347	0
38:2c:4a:6e:19:6b	01:00:5e:00:00:16	5	270	5	270	0	0	285.27955	0.4311	5010	0
b8:27:eb:39:d3:5b	00:0c:29:16:ae:a4	4,374	283 k	2,911	187 k	1,463	96 k	1.681942	362.2161	4145	2125
b8:27:eb:3b:4c:2d	00:0c:29:16:ae:a4	4,375	283 k	2,911	187 k	1,464	96 k	1.681511	362.1934	4145	2126
b8:27:eb:51:6e:81	00:0c:29:16:ae:a4	4,376	284 k	2,912	187 k	1,464	96 k	1.681512	362.2228	4146	2126
b8:27:eb:c5:9c:b5	00:0c:29:16:ae:a4	4,374	283 k	2,910	187 k	1,464	96 k	1.681941	362.2708	4143	2126

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

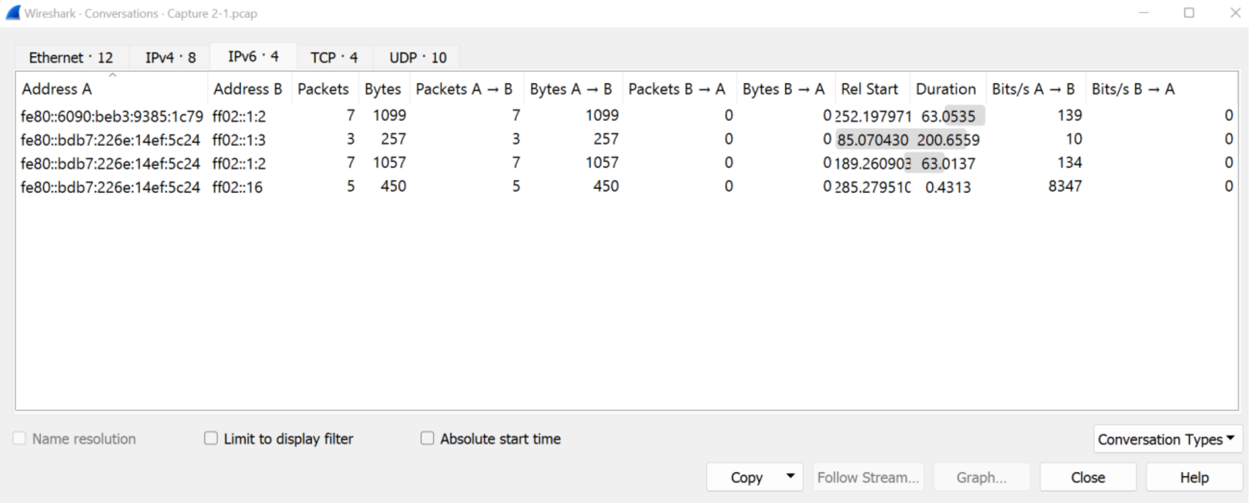
Figure 2(d1): MAC addresses fetched from conversations in Statistics of Capture file in Wireshark



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.192.50	172.16.255.255	3	276	3	276	0	0	84.653080	1.4956	1476	0
172.16.192.50	224.0.0.252	3	197	3	197	0	0	85.070560	200.6559	7	0
172.16.192.50	224.0.0.22	5	270	5	270	0	0	285.27955	0.4311	5010	0
172.16.192.200	172.16.255.255	6	552	6	552	0	0	0.000000	10.5917	416	0
172.16.192.200	172.16.192.30	4,348	282 k	1,451	95 k	2,897	186 k	1.681684	362.1932	2114	4127
172.16.192.200	172.16.192.31	4,349	282 k	1,451	95 k	2,898	186 k	1.681734	362.2226	2114	4128
172.16.192.200	172.16.192.32	4,347	282 k	1,451	95 k	2,896	186 k	1.682541	362.2702	2114	4124
172.16.192.200	172.16.192.33	4,347	282 k	1,450	95 k	2,897	186 k	1.682589	362.2154	2113	4126

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Figure 2(d2): Example IPV4 Address that have bidirectional communication with the MAC address



Wireshark · Conversations · Capture 2-1.pcap

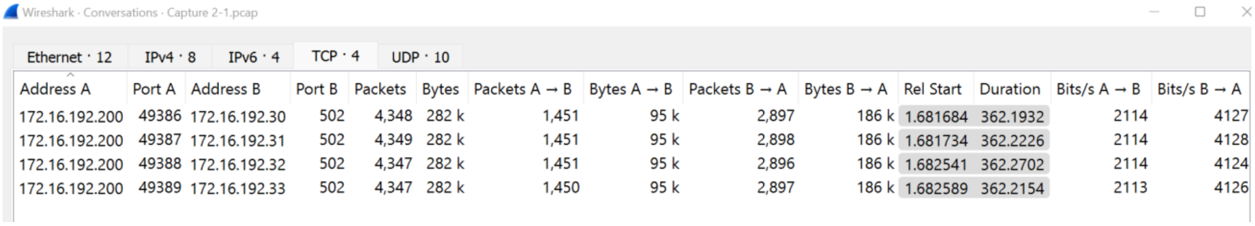
Ethernet · 12 | IPv4 · 8 | IPv6 · 4 | TCP · 4 | UDP · 10

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
fe80::6090:beb3:9385:1c79	ff02::1:2	7	1099	7	1099	0	0	252.197971	63.0535	139	0
fe80::bdb7:226e:14ef:5c24	ff02::1:3	3	257	3	257	0	0	85.070430	200.6559	10	0
fe80::bdb7:226e:14ef:5c24	ff02::1:2	7	1057	7	1057	0	0	189.26090	63.0137	134	0
fe80::bdb7:226e:14ef:5c24	ff02::16	5	450	5	450	0	0	285.27951	0.4313	8347	0

Figure 2(d3): Example IPV6 Address that have bidirectional communication with the MAC address

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?

Answer: There is only one IP address that interacts with multiple devices in the network, which has either the inbound or outbound communication. The IP address is 172.16.192.200. Please refer the sample figures 2(e1), figures 2(e2), figures 2(e3), figures 2(e4).

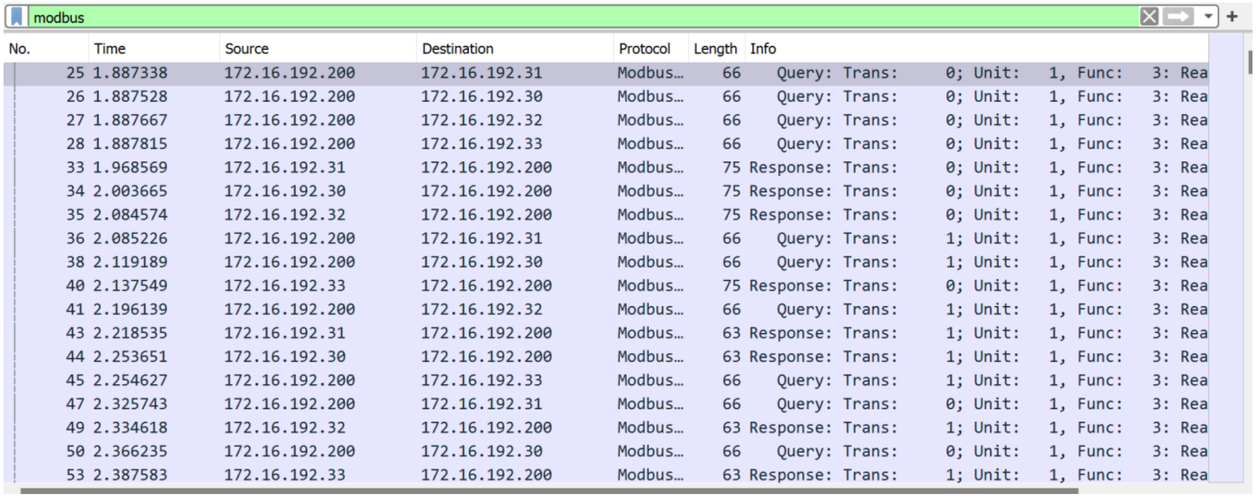


Wireshark · Conversations · Capture 2-1.pcap

Ethernet · 12 | IPv4 · 8 | IPv6 · 4 | TCP · 4 | UDP · 10

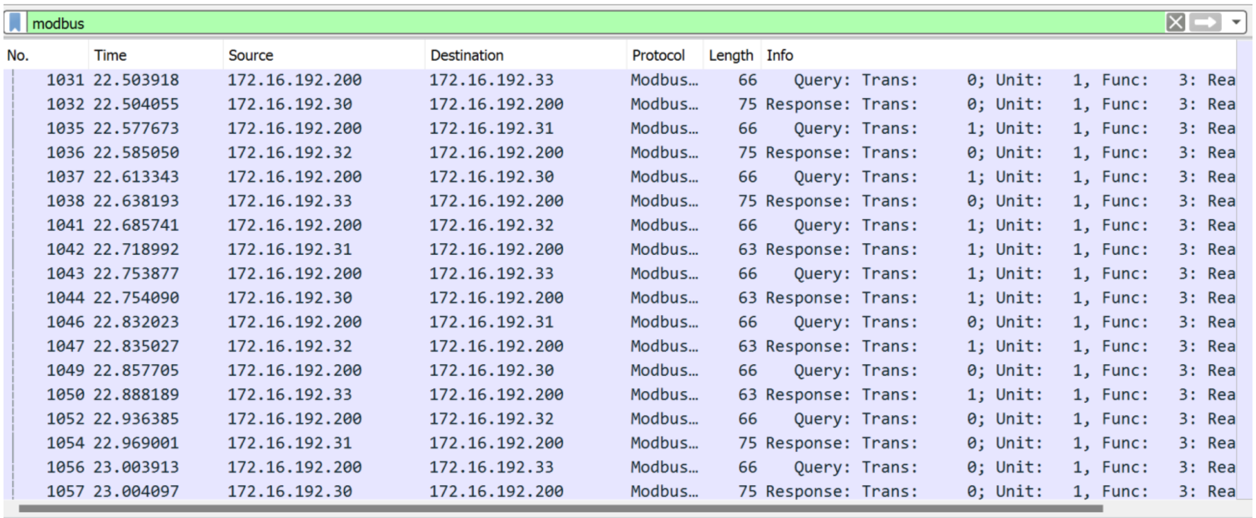
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.192.200	49386	172.16.192.30	502	4,348	282 k	1,451	95 k	2,897	186 k	1.681684	362.1932	2114	4127
172.16.192.200	49387	172.16.192.31	502	4,349	282 k	1,451	95 k	2,898	186 k	1.681734	362.2226	2114	4128
172.16.192.200	49388	172.16.192.32	502	4,347	282 k	1,451	95 k	2,896	186 k	1.682541	362.2702	2114	4124
172.16.192.200	49389	172.16.192.33	502	4,347	282 k	1,450	95 k	2,897	186 k	1.682589	362.2154	2113	4126

Figure 2(e1):IP address of Server



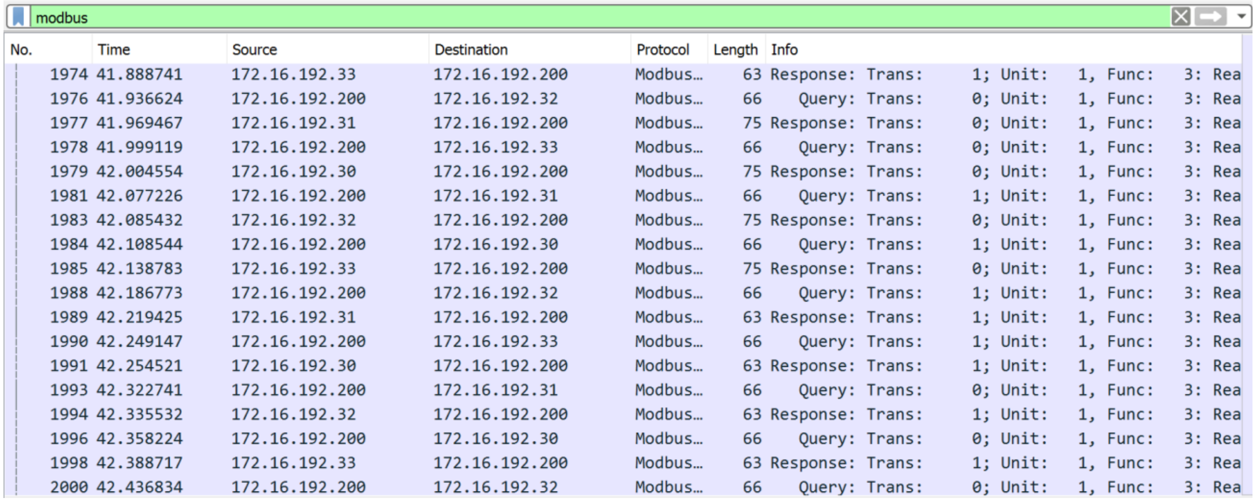
```
modbus
No.   Time      Source           Destination      Protocol  Length  Info
   25 1.887338  172.16.192.200   172.16.192.31    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
   26 1.887528  172.16.192.200   172.16.192.30    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
   27 1.887667  172.16.192.200   172.16.192.32    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
   28 1.887815  172.16.192.200   172.16.192.33    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
   33 1.968569  172.16.192.31    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
   34 2.003665  172.16.192.30    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
   35 2.084574  172.16.192.32    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
   36 2.085226  172.16.192.200   172.16.192.31    Modbus…   66     Query: Trans:    1; Unit:   1, Func:   3: Rea
   38 2.119189  172.16.192.200   172.16.192.30    Modbus…   66     Query: Trans:    1; Unit:   1, Func:   3: Rea
   40 2.137549  172.16.192.33    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
   41 2.196139  172.16.192.200   172.16.192.32    Modbus…   66     Query: Trans:    1; Unit:   1, Func:   3: Rea
   43 2.218535  172.16.192.31    172.16.192.200   Modbus…   63  Response: Trans:    1; Unit:   1, Func:   3: Rea
   44 2.253651  172.16.192.30    172.16.192.200   Modbus…   63  Response: Trans:    1; Unit:   1, Func:   3: Rea
   45 2.254627  172.16.192.200   172.16.192.33    Modbus…   66     Query: Trans:    1; Unit:   1, Func:   3: Rea
   47 2.325743  172.16.192.200   172.16.192.31    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
   49 2.334618  172.16.192.32    172.16.192.200   Modbus…   63  Response: Trans:    1; Unit:   1, Func:   3: Rea
   50 2.366235  172.16.192.200   172.16.192.30    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
   53 2.387583  172.16.192.33    172.16.192.200   Modbus…   63  Response: Trans:    1; Unit:   1, Func:   3: Rea
```

Figure 2(e2): Modbus IP addresses of Server



```
modbus
No.   Time       Source           Destination      Protocol  Length  Info
 1031 22.503918  172.16.192.200   172.16.192.33    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
 1032 22.504055  172.16.192.30    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
 1035 22.577673  172.16.192.200   172.16.192.31    Modbus…   66     Query: Trans:    1; Unit:   1, Func:   3: Rea
 1036 22.585050  172.16.192.32    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
 1037 22.613343  172.16.192.200   172.16.192.30    Modbus…   66     Query: Trans:    1; Unit:   1, Func:   3: Rea
 1038 22.638193  172.16.192.33    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
 1041 22.685741  172.16.192.200   172.16.192.32    Modbus…   66     Query: Trans:    1; Unit:   1, Func:   3: Rea
 1042 22.718992  172.16.192.31    172.16.192.200   Modbus…   63  Response: Trans:    1; Unit:   1, Func:   3: Rea
 1043 22.753877  172.16.192.200   172.16.192.33    Modbus…   66     Query: Trans:    1; Unit:   1, Func:   3: Rea
 1044 22.754090  172.16.192.30    172.16.192.200   Modbus…   63  Response: Trans:    1; Unit:   1, Func:   3: Rea
 1046 22.832023  172.16.192.200   172.16.192.31    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
 1047 22.835027  172.16.192.32    172.16.192.200   Modbus…   63  Response: Trans:    1; Unit:   1, Func:   3: Rea
 1049 22.857705  172.16.192.200   172.16.192.30    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
 1050 22.888189  172.16.192.33    172.16.192.200   Modbus…   63  Response: Trans:    1; Unit:   1, Func:   3: Rea
 1052 22.936385  172.16.192.200   172.16.192.32    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
 1054 22.969001  172.16.192.31    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
 1056 23.003913  172.16.192.200   172.16.192.33    Modbus…   66     Query: Trans:    0; Unit:   1, Func:   3: Rea
 1057 23.004097  172.16.192.30    172.16.192.200   Modbus…   75  Response: Trans:    0; Unit:   1, Func:   3: Rea
```

Figure 2(e3): Modbus IP addresses of Server



modbus

No.	Time	Source	Destination	Protocol	Length	Info
1974	41.888741	172.16.192.33	172.16.192.200	Modbus…	63	Response: Trans: 1; Unit: 1, Func: 3: Rea
1976	41.936624	172.16.192.200	172.16.192.32	Modbus…	66	Query: Trans: 0; Unit: 1, Func: 3: Rea
1977	41.969467	172.16.192.31	172.16.192.200	Modbus…	75	Response: Trans: 0; Unit: 1, Func: 3: Rea
1978	41.999119	172.16.192.200	172.16.192.33	Modbus…	66	Query: Trans: 0; Unit: 1, Func: 3: Rea
1979	42.004554	172.16.192.30	172.16.192.200	Modbus…	75	Response: Trans: 0; Unit: 1, Func: 3: Rea
1981	42.077226	172.16.192.200	172.16.192.31	Modbus…	66	Query: Trans: 1; Unit: 1, Func: 3: Rea
1983	42.085432	172.16.192.32	172.16.192.200	Modbus…	75	Response: Trans: 0; Unit: 1, Func: 3: Rea
1984	42.108544	172.16.192.200	172.16.192.30	Modbus…	66	Query: Trans: 1; Unit: 1, Func: 3: Rea
1985	42.138783	172.16.192.33	172.16.192.200	Modbus…	75	Response: Trans: 0; Unit: 1, Func: 3: Rea
1988	42.186773	172.16.192.200	172.16.192.32	Modbus…	66	Query: Trans: 1; Unit: 1, Func: 3: Rea
1989	42.219425	172.16.192.31	172.16.192.200	Modbus…	63	Response: Trans: 1; Unit: 1, Func: 3: Rea
1990	42.249147	172.16.192.200	172.16.192.33	Modbus…	66	Query: Trans: 1; Unit: 1, Func: 3: Rea
1991	42.254521	172.16.192.30	172.16.192.200	Modbus…	63	Response: Trans: 1; Unit: 1, Func: 3: Rea
1993	42.322741	172.16.192.200	172.16.192.31	Modbus…	66	Query: Trans: 0; Unit: 1, Func: 3: Rea
1994	42.335532	172.16.192.32	172.16.192.200	Modbus…	63	Response: Trans: 1; Unit: 1, Func: 3: Rea
1996	42.358224	172.16.192.200	172.16.192.30	Modbus…	66	Query: Trans: 0; Unit: 1, Func: 3: Rea
1998	42.388717	172.16.192.33	172.16.192.200	Modbus…	63	Response: Trans: 1; Unit: 1, Func: 3: Rea
2000	42.436834	172.16.192.200	172.16.192.32	Modbus…	66	Query: Trans: 0; Unit: 1, Func: 3: Rea

Figure 2(e4): Modbus IP addresses of Server

Task (2)

(1) Sign up for a free account at www.shodan.io. Note that the registration is free but access to some sensitive information needs payment. You do NOT need to pay the website.

(2) Login to Shodan. Click “explore” at the top. You will see several hot categories. See the attached screenshot.

(3) You can directly type “port:502” in the top explore window. You will then see many items shown on the screen. They are IoT devices that you can access all around the world. You can choose one country or one organization to explore.

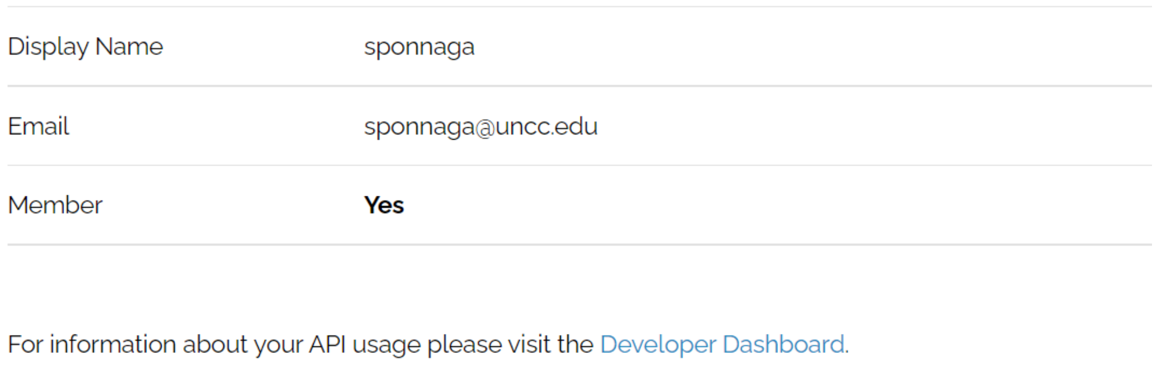
(4) Now find one device/IP address returned by shodan that does not show “error” or illegal device type. You can see from the summary what type of device it is. Use google to find out the device type, its manual, and any vulnerabilities associated with the device. This is usually how attackers locate targets and vulnerabilities.

Turn-ins: For task 1, answer all questions and write a paragraph to describe how you figure out the shared MAC address that is associated with multiple IP addresses. Attach at least three screenshots to show how to finish the task. Do not share your screenshots with other students.

For task 2, show the screenshot of the IP address and device type that you find in shodan. Also write a half page report on any vulnerabilities that you can find for this device/chip. If you cannot find any vulnerability report for the device, change to another one.

Tip: Wireshark can run on both Windows and Linux machines. I believe there are wiretap tools for Mac as well. In Windows, when you start Wireshark and if you see “no interface can be found”, close the application, right click “WireShark”, choose “Run as administrator” and you should be fine.

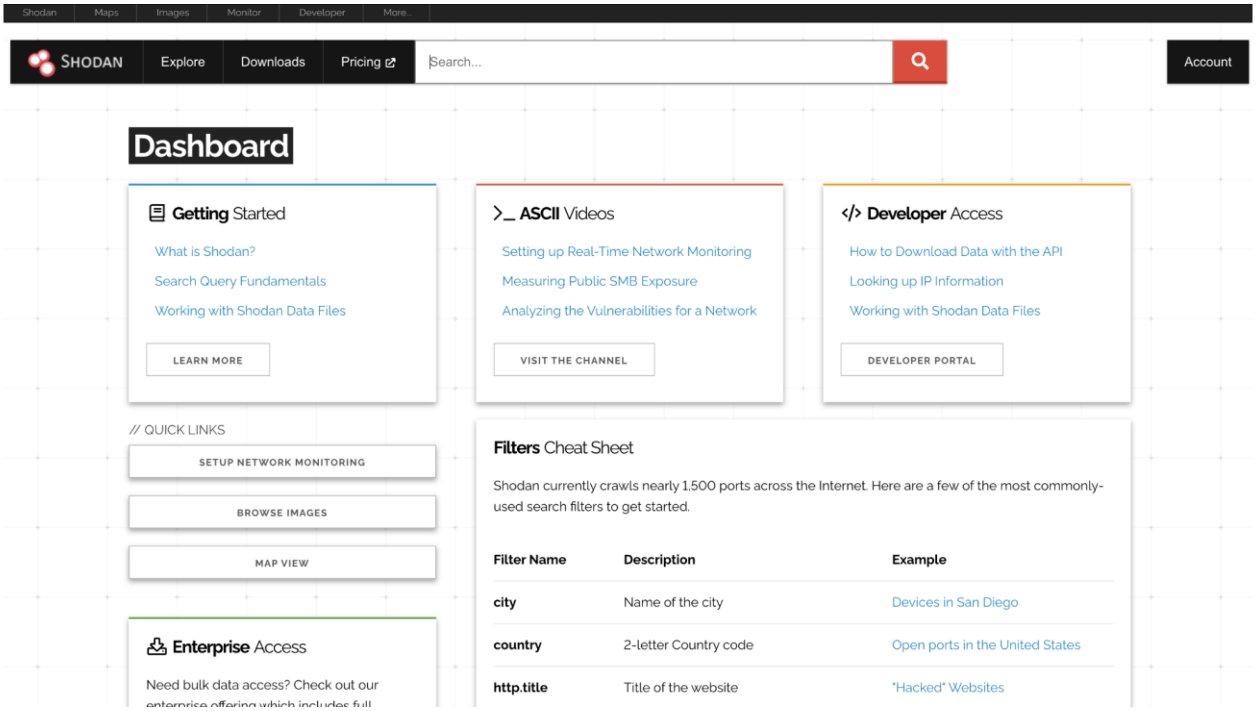
The following figure shows a screenshot from Shodan. At the IP address 149.28.9.121, you can find many open ports. The device type is Siemens SIMATIC S7-200. Through google, you can find that it is a Siemens Programmable Controller that uses Modbus protocol. You can then find any vulnerabilities associated with the device or protocol. Note that Shodan also shows the physical zone (Seattle area). We also provide a few screenshots for locating the devices in Shodan.



Display Name	sponnaga
Email	sponnaga@uncc.edu
Member	**Yes**

For information about your API usage please visit the Developer Dashboard.

Figure 2.1 : Signed up to Shodan Account



Dashboard

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

// QUICK LINKS

SETUP NETWORK MONITORING

BROWSE IMAGES

MAP VIEW

Enterprise Access

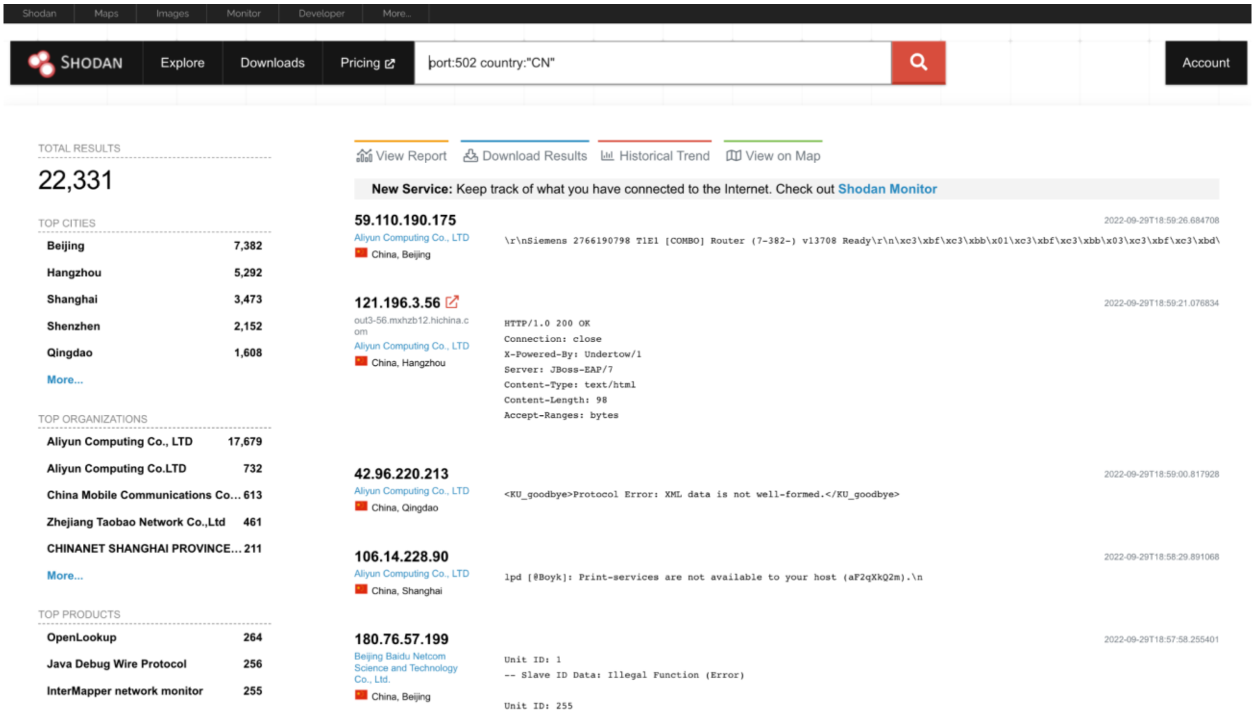
Need bulk data access? Check out our enterprise offering which includes full

Filters Cheat Sheet

Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego
country	2-letter Country code	Open ports in the United States
http.title	Title of the website	"Hacked" Websites

Figure 2.2:Logged in Shodan



port:502 country:"CN"

TOTAL RESULTS

22,331

TOP CITIES

Beijing	7,382
Hangzhou	5,292
Shanghai	3,473
Shenzhen	2,152
Qingdao	1,608

More...

TOP ORGANIZATIONS

Aliyun Computing Co., LTD	17,679
Aliyun Computing Co.LTD	732
China Mobile Communications Co...	613
Zhejiang Taobao Network Co.,Ltd	461
CHINANET SHANGHAI PROVINCE...	211

More...

TOP PRODUCTS

OpenLookup	264
Java Debug Wire Protocol	256
InterMapper network monitor	255

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

59.110.190.175
Aliyun Computing Co., LTD
China, Beijing
2022-09-29T18:59:26.684708

```
\r\nSiemens 2766190798 T1E1 [COMBO] Router (7-382-) v13708 Ready\r\n\xc3\xbf\xc3\xbb\x01\xc3\xbf\xc3\xbb\x03\xc3\xbf\xc3\xbd\
```

121.196.3.56
out3-56.mxhzb12.hichina.com
Aliyun Computing Co., LTD
China, Hangzhou
2022-09-29T18:59:21.076834

```
HTTP/1.0 200 OK
Connection: close
X-Powered-By: Undertow/1
Server: JBoss-EAP/7
Content-Type: text/html
Content-Length: 98
Accept-Ranges: bytes
```

42.96.220.213
Aliyun Computing Co., LTD
China, Qingdao
2022-09-29T18:59:00.817928

```
<KU_goodbye>Protocol Error: XML data is not well-formed.</KU_goodbye>
```

106.14.228.90
Aliyun Computing Co., LTD
China, Shanghai
2022-09-29T18:58:29.891068

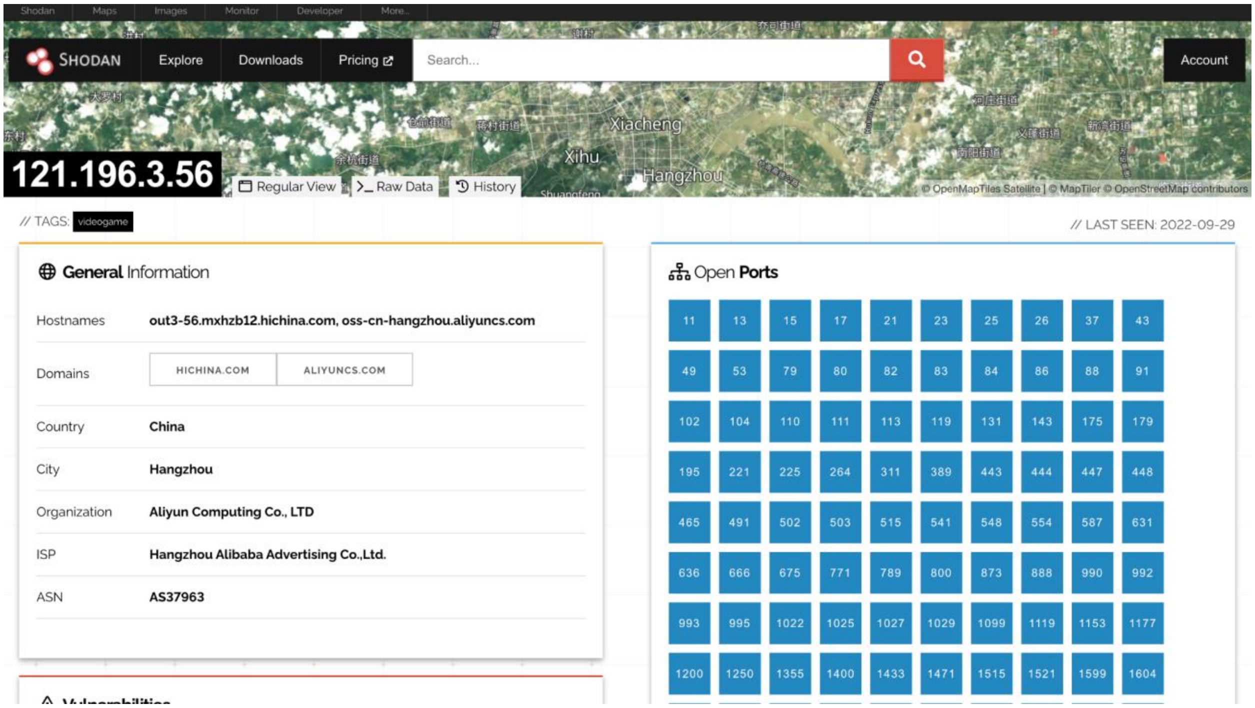
```
lpd [@Boyk]: Print-services are not available to your host (aF2qXkQ2m).\n
```

180.76.57.199
Beijing Baidu Netcom Science and Technology Co., Ltd.
China, Beijing
2022-09-29T18:57:58.255401

```
Unit ID: 1
-- Slave ID Data: Illegal Function (Error)

Unit ID: 255
```

Figure 2.3 Search for Port 502



121.196.3.56

// TAGS: videogame

// LAST SEEN: 2022-09-29

General Information

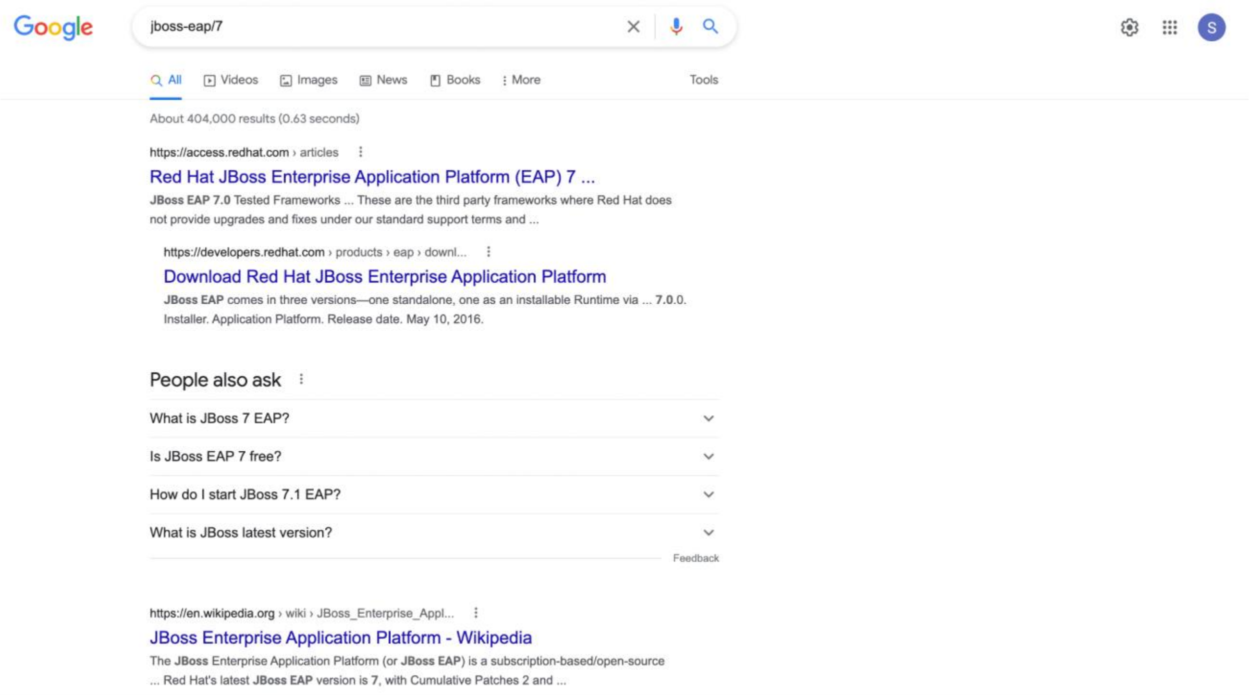
Hostnames	out3-56.mxhzb12.hichina.com, oss-cn-hangzhou.aliyuncs.com
Domains	HICHINA.COM ALIYUNCS.COM
Country	China
City	Hangzhou
Organization	Aliyun Computing Co., LTD
ISP	Hangzhou Alibaba Advertising Co.,Ltd.
ASN	AS37963

Open **Ports**

```
11   13   15   17   21   23   25   26   37   43
49   53   79   80   82   83   84   86   88   91
102  104  110  111  113  119  131  143  175  179
195  221  225  264  311  389  443  444  447  448
465  491  502  503  515  541  548  554  587  631
636  666  675  771  789  800  873  888  990  992
993  995  1022 1025 1027 1029 1099 1119 1153 1177
1200 1250 1355 1400 1433 1471 1515 1521 1599 1604
```

Vulnerabilities

Figure 2.4 Locate a device of interest



jboss-eap/7

About 404,000 results (0.63 seconds)

https://access.redhat.com › articles

Red Hat JBoss Enterprise Application Platform (EAP) 7 ...

JBoss EAP 7.0 Tested Frameworks ... These are the third party frameworks where Red Hat does not provide upgrades and fixes under our standard support terms and ...

https://developers.redhat.com › products › eap › downl...

Download Red Hat JBoss Enterprise Application Platform

JBoss EAP comes in three versions—one standalone, one as an installable Runtime via ... **7.0**.0. Installer. Application Platform. Release date. May 10, 2016.

People also ask

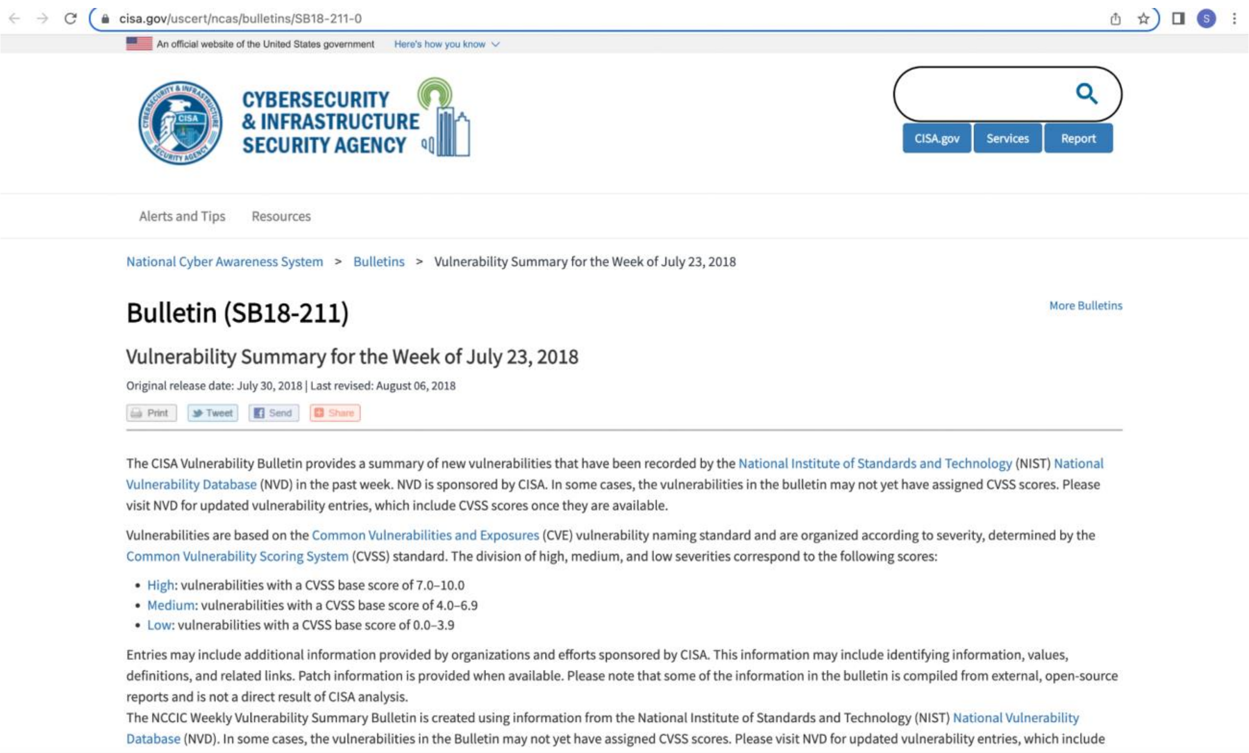
- What is JBoss 7 EAP?
- Is JBoss EAP 7 free?
- How do I start JBoss 7.1 EAP?
- What is JBoss latest version?

https://en.wikipedia.org › wiki › JBoss_Enterprise_Appl...

JBoss Enterprise Application Platform - Wikipedia

The **JBoss** Enterprise Application Platform (or **JBoss EAP**) is a subscription-based/open-source ... Red Hat's latest **JBoss EAP** version is **7**, with Cumulative Patches 2 and ...

Figure 2.4(a): Searching the Device name in google to check vulnerabilities



cisa.gov/uscert/ncas/bulletins/SB18-211-0
An official website of the United States government
Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA.gov
Services
Report
Alerts and Tips
Resources
Print
Tweet
Send
Share
More Bulletins

National Cyber Awareness System > Bulletins > Vulnerability Summary for the Week of July 23, 2018

Bulletin (SB18-211)

Vulnerability Summary for the Week of July 23, 2018

Original release date: July 30, 2018 | Last revised: August 06, 2018

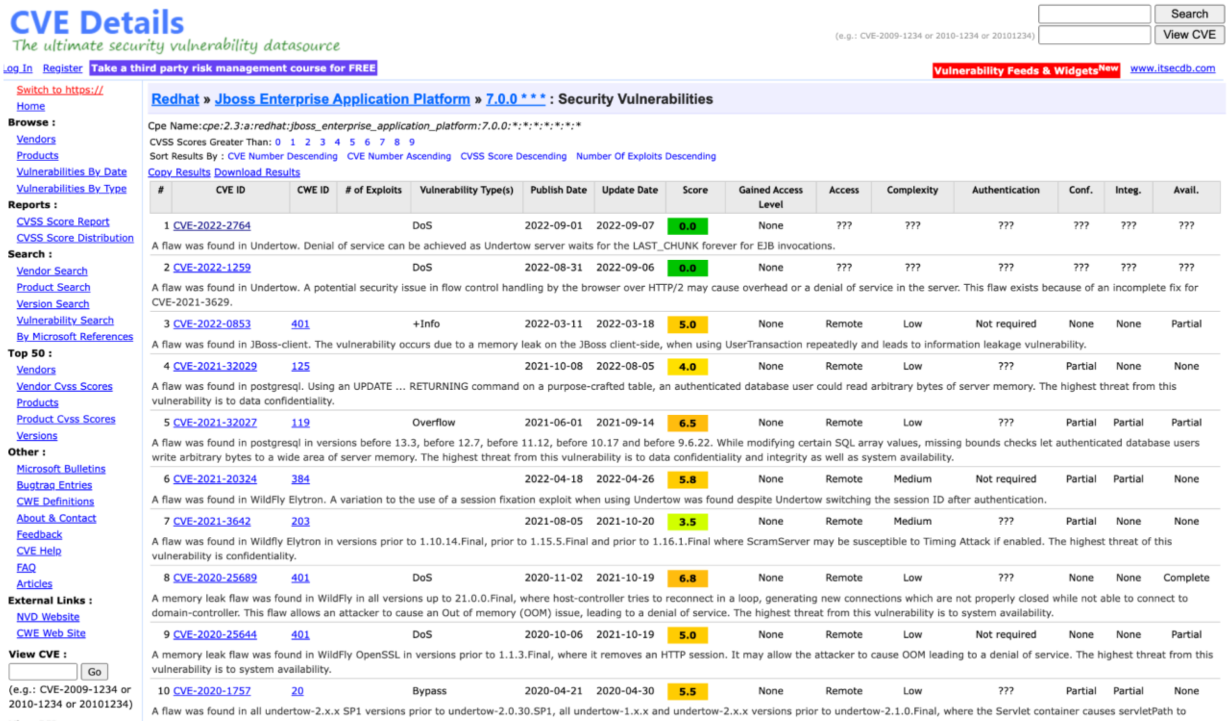
The CISA Vulnerability Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. NVD is sponsored by CISA. In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

Vulnerabilities are based on the Common Vulnerabilities and Exposures (CVE) vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- High: vulnerabilities with a CVSS base score of 7.0–10.0
- Medium: vulnerabilities with a CVSS base score of 4.0–6.9
- Low: vulnerabilities with a CVSS base score of 0.0–3.9

Entries may include additional information provided by organizations and efforts sponsored by CISA. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletin is compiled from external, open-source reports and is not a direct result of CISA analysis.
The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include

Figure 2.4(b):Search for specific devices and vulnerabilities in CISA



Redhat » Jboss Enterprise Application Platform » 7.0.0 * * * : Security Vulnerabilities

Cpe Name:*cpe:2.3:a:redhat:jboss_enterprise_application_platform:7.0.0:*:*:*:*:*:*:**

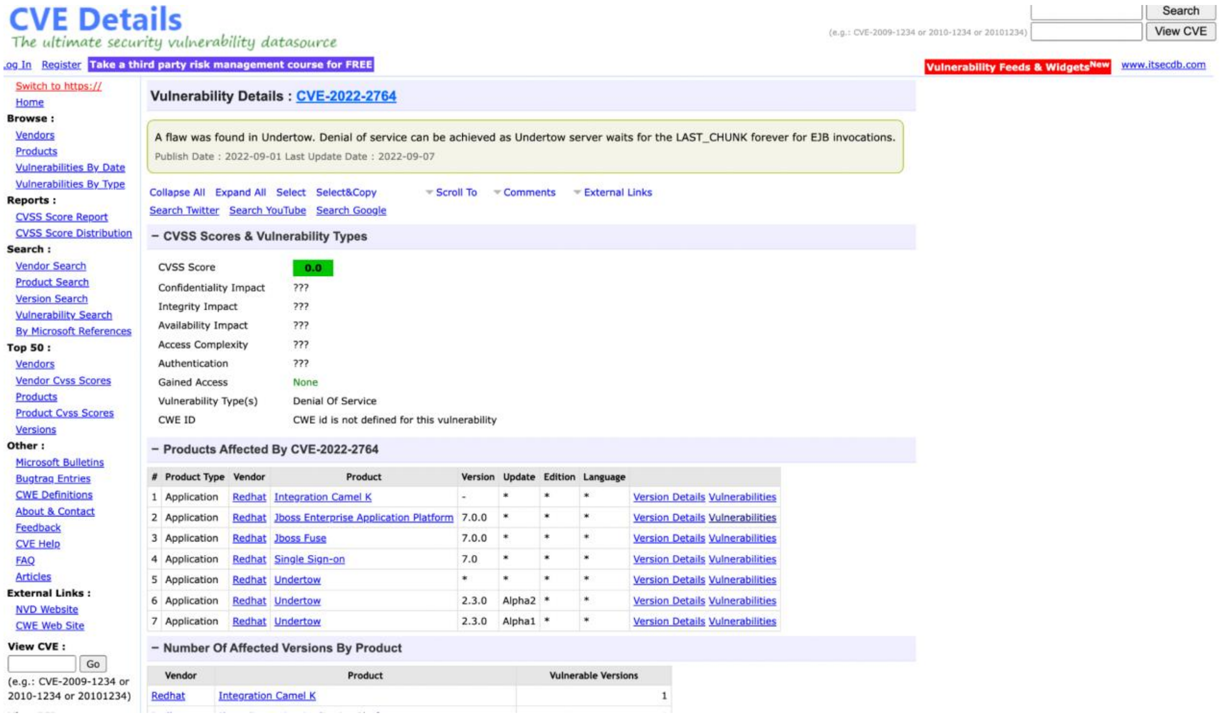
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th><th>Avail.</th></tr>
<tr><td>1</td><td>CVE-2022-2764</td><td></td><td></td><td>DoS</td><td>2022-09-01</td><td>2022-09-07</td><td>0.0</td><td>None</td><td>???</td><td>???</td><td>???</td><td>???</td><td>???</td><td>???</td></tr>
<tr><td colspan="15">A flaw was found in Undertow. Denial of service can be achieved as Undertow server waits for the LAST_CHUNK forever for EJB invocations.</td></tr>
<tr><td>2</td><td>CVE-2022-1259</td><td></td><td></td><td>DoS</td><td>2022-08-31</td><td>2022-09-06</td><td>0.0</td><td>None</td><td>???</td><td>???</td><td>???</td><td>???</td><td>???</td><td>???</td></tr>
<tr><td colspan="15">A flaw was found in Undertow. A potential security issue in flow control handling by the browser over HTTP/2 may cause overhead or a denial of service in the server. This flaw exists because of an incomplete fix for CVE-2021-3629.</td></tr>
<tr><td>3</td><td>CVE-2022-0853</td><td>401</td><td></td><td>+Info</td><td>2022-03-11</td><td>2022-03-18</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">A flaw was found in JBoss-client. The vulnerability occurs due to a memory leak on the JBoss client-side, when using UserTransaction repeatedly and leads to information leakage vulnerability.</td></tr>
<tr><td>4</td><td>CVE-2021-32029</td><td>125</td><td></td><td></td><td>2021-10-08</td><td>2022-08-05</td><td>4.0</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Partial</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">A flaw was found in postgresql. Using an UPDATE ... RETURNING command on a purpose-crafted table, an authenticated database user could read arbitrary bytes of server memory. The highest threat from this vulnerability is to data confidentiality.</td></tr>
<tr><td>5</td><td>CVE-2021-32027</td><td>119</td><td></td><td>Overflow</td><td>2021-06-01</td><td>2021-09-14</td><td>6.5</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Partial</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="15">A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.</td></tr>
<tr><td>6</td><td>CVE-2021-20324</td><td>384</td><td></td><td></td><td>2022-04-18</td><td>2022-04-26</td><td>5.8</td><td>None</td><td>Remote</td><td>Medium</td><td>Not required</td><td>Partial</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">A flaw was found in WildFly Elytron. A variation to the use of a session fixation exploit when using Undertow was found despite Undertow switching the session ID after authentication.</td></tr>
<tr><td>7</td><td>CVE-2021-3642</td><td>203</td><td></td><td></td><td>2021-08-05</td><td>2021-10-20</td><td>3.5</td><td>None</td><td>Remote</td><td>Medium</td><td>???</td><td>Partial</td><td>None</td><td>None</td></tr>
<tr><td colspan="15">A flaw was found in Wildfly Elytron in versions prior to 1.10.14.Final, prior to 1.15.5.Final and prior to 1.16.1.Final where ScramServer may be susceptible to Timing Attack if enabled. The highest threat of this vulnerability is confidentiality.</td></tr>
<tr><td>8</td><td>CVE-2020-25689</td><td>401</td><td></td><td>DoS</td><td>2020-11-02</td><td>2021-10-19</td><td>6.8</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>None</td><td>None</td><td>Complete</td></tr>
<tr><td colspan="15">A memory leak flaw was found in WildFly in all versions up to 21.0.0.Final, where host-controller tries to reconnect in a loop, generating new connections which are not properly closed while not able to connect to domain-controller. This flaw allows an attacker to cause an Out of memory (OOM) issue, leading to a denial of service. The highest threat from this vulnerability is to system availability.</td></tr>
<tr><td>9</td><td>CVE-2020-25644</td><td>401</td><td></td><td>DoS</td><td>2020-10-06</td><td>2021-10-19</td><td>5.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>None</td><td>None</td><td>Partial</td></tr>
<tr><td colspan="15">A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability.</td></tr>
<tr><td>10</td><td>CVE-2020-1757</td><td>20</td><td></td><td>Bypass</td><td>2020-04-21</td><td>2020-04-30</td><td>5.5</td><td>None</td><td>Remote</td><td>Low</td><td>???</td><td>Partial</td><td>Partial</td><td>None</td></tr>
<tr><td colspan="15">A flaw was found in all undertow-2.x.x SP1 versions prior to undertow-2.0.30.SP1, all undertow-1.x.x and undertow-2.x.x versions prior to undertow-2.1.0.Final, where the Servlet container causes servletPath to</td></tr>
</table>

Figure 2.4(c): Checking all the vulnerabilities of the device jboss-eap



Vulnerability Details : CVE-2022-2764

A flaw was found in Undertow. Denial of service can be achieved as Undertow server waits for the LAST_CHUNK forever for EJB invocations.

Publish Date : 2022-09-01 Last Update Date : 2022-09-07

− CVSS Scores & Vulnerability Types

CVSS Score	0.0
Confidentiality Impact	???
Integrity Impact	???
Availability Impact	???
Access Complexity	???
Authentication	???
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

− Products Affected By CVE-2022-2764

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Redhat	Integration Camel K	-	*	*	*	Version Details Vulnerabilities
2	Application	Redhat	Jboss Enterprise Application Platform	7.0.0	*	*	*	Version Details Vulnerabilities
3	Application	Redhat	Jboss Fuse	7.0.0	*	*	*	Version Details Vulnerabilities
4	Application	Redhat	Single Sign-on	7.0	*	*	*	Version Details Vulnerabilities
5	Application	Redhat	Undertow	*	*	*	*	Version Details Vulnerabilities
6	Application	Redhat	Undertow	2.3.0	Alpha2	*	*	Version Details Vulnerabilities
7	Application	Redhat	Undertow	2.3.0	Alpha1	*	*	Version Details Vulnerabilities

− Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Redhat	Integration Camel K	1

Figure 2.4(d): CVE details of vulnerability CVE-2022-2764

Vulnerabilities:

Name of Vulnerability: CVE – 2018- 15919 Detail

Severity: Base Score = 5.3 Medium

Description:

The Remote attackers may observe the targeted users behavior in OpenSSH versions 7.8 and previous to them with the help of the auth-gss2.c whenever the GSS2 is in ON state. Even Though the username enumeration happens, this will be considered as a zero-day exploit.

The SUSE SLES11 Security Update: openssh (SUSE-SU-2018:3540-1) plugin from the vulnerability scanner Nessus assists in locating the vulnerability in a target environment. It is operating in the local environment and belongs to the SuSE Local Security Checks family. This flaw can be tested with plugin 171714 for SUSE Enterprise Linux Security Update for openssh (SUSE-SU-2018:3781-1) by the for-profit vulnerability scanner Qualys.

For example, When the username is correct but the password is incorrect, there are different messages than when the username is valid but the password is incorrect. By experimenting with different values until the notification about the invalid password is received, a potential attacker can exploit this difference to understand the current state of the login function and possibly find a valid username. In essence, this facilitates an attacker's acquisition of the other half of the required authentication credentials.

Although a user may find this kind of information beneficial, a potential attacker may also find it interesting. The message for both unsuccessful scenarios in the aforementioned example should be the same.

Reference:

vuldb(2020, March 19). OPENSSH UP TO 7.8 GSS2 AUTH-GSS2.C USERNAME INFORMATION DISCLOSURE. https://vuldb.com/?id.123343

National Vulnerability Database(2019, March 7). CVE-2018-15919 Detail. https://nvd.nist.gov/vuln/detail/CVE-2018-15919

Common Wellness Enumeration(n.d). CWE-200: Exposure of Sensitive Information to an Unauthorized Actor. https://cwe.mitre.org/data/definitions/200.html