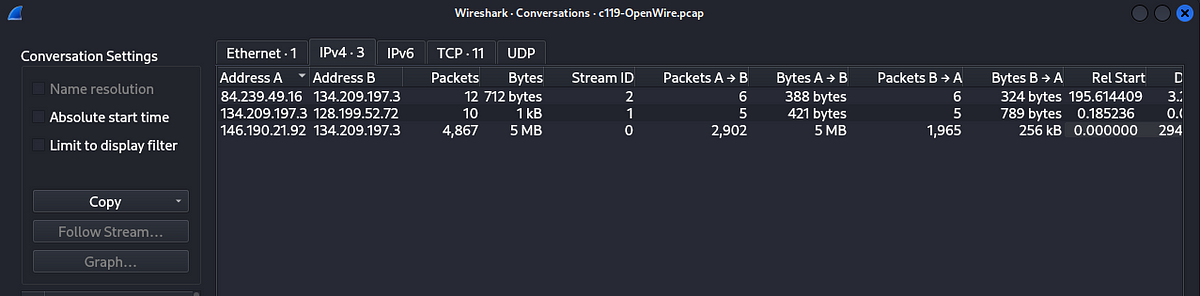
### **OpenWire — CyberDefenders**

**Scenario:** During your shift as a tier-2 SOC analyst, you receive an escalation from a tier-1 analyst regarding a public-facing server. This server has been flagged for making outbound connections to multiple suspicious IPs. In response, you initiate the standard incident response protocol, which includes isolating the server from the network to prevent potential lateral movement or data exfiltration and obtaining a packet capture from the NSM utility for analysis. Your task is to analyze the pcap and assess for signs of malicious activity.

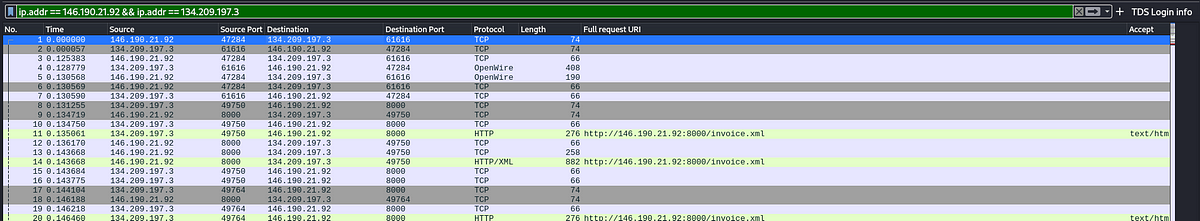
#### **Tasks**

1. By identifying the C2 IP, we can block traffic to and from this IP, helping to contain the breach and prevent further data exfiltration or command execution. Can you provide the IP of the C2 server that communicated with our server?

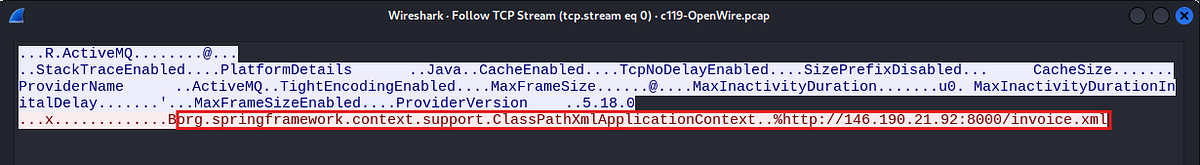
Examine the conversations tab in Wireshark.



We can see above, there are four hosts in this capture file. Also we can notice that the IP addresses 146[.]190[.]21[.]92 and 134[.]209[.]197[.]3 have the most number of packets between them. Let us examine the traffic between these two IP addresses.



Let us examine the packets, let us see the first packet in this traffic. Follow the TCP stream on the first packet displayed.

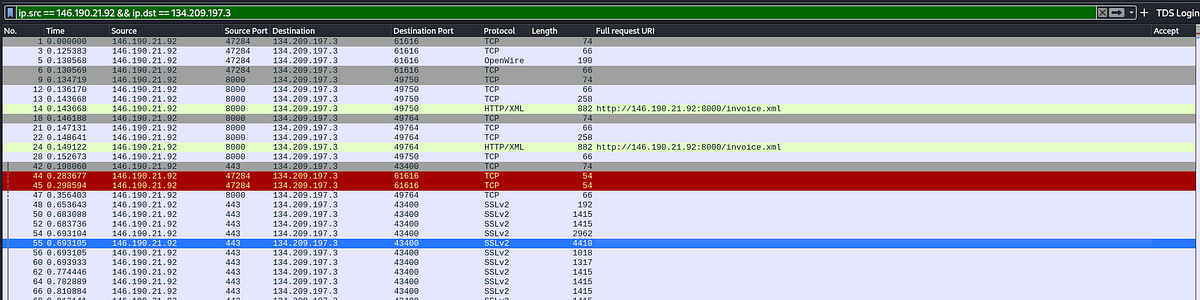


We can see that it has a code that will load an XML file from a remote server. This code is usually used to load spring configuration files.

Answer: 146[.]190[.]21[.]92

2. Initial entry points are critical to trace back the attack vector. What is the port number of the service the adversary exploited?

Filter the traffic, where the source IP address is 146[.]190[.]21[.]92 and the destination address is 134[.]209[.]197[.]3.



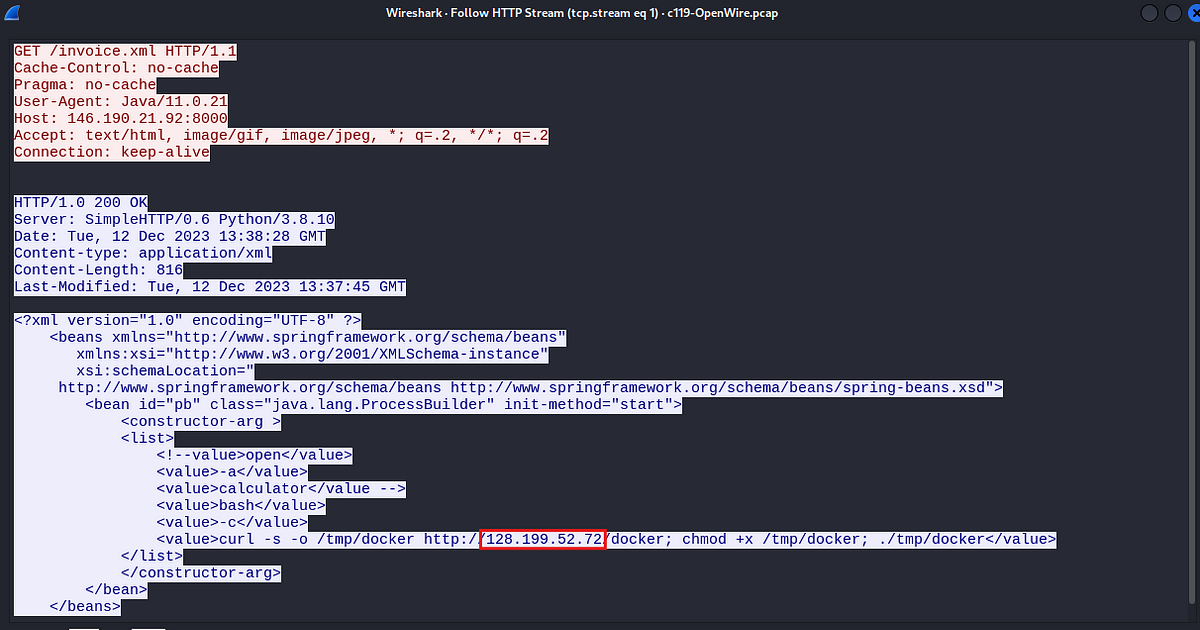
We can see above, the port used to initially contact the victim.

Answer: 61616

3. Following up on the previous question, what is the name of the service found to be vulnerable?  
The above discovered port is a default port for OpenWire protocol which is a communication protocol used by ActiveMQ which facilitates communication between applications.

Answer: Apache ActiveMQ

4. The attacker’s infrastructure often involves multiple components. What is the IP of the second C2 server?  
Let us examine the XML file that the attacker downloaded on to the server.



We can see above that this file is downloading another file from a different IP address. This IP address will be the answer for this question.

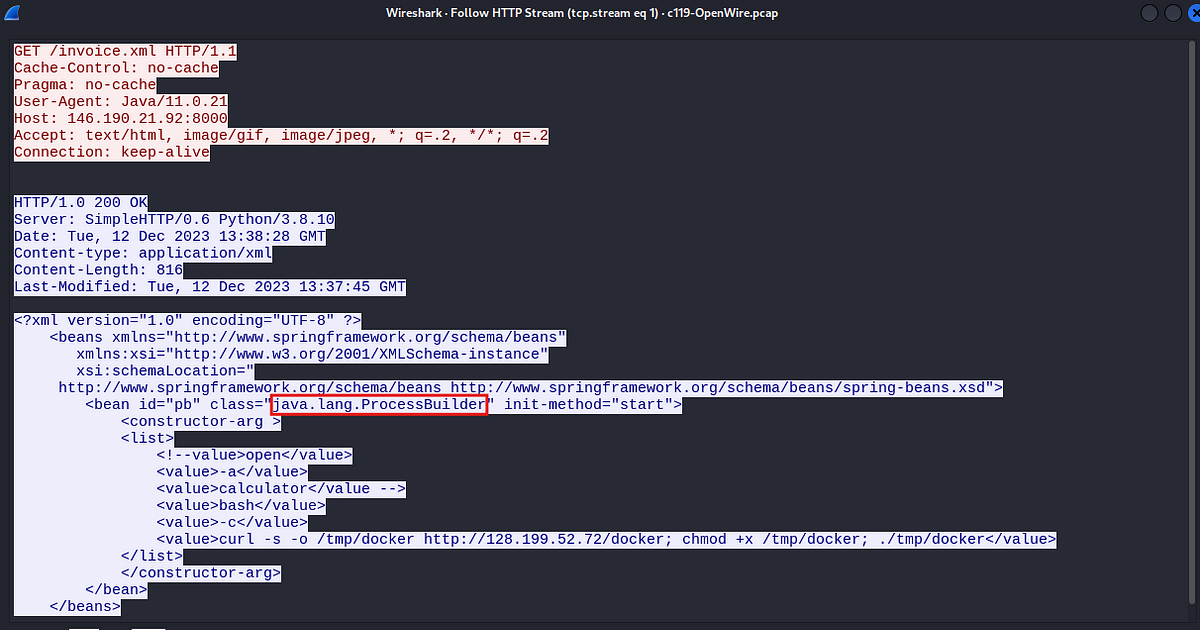
Answer: 128[.]199[.]52[.]72

5. Attackers usually leave traces on the disk. What is the name of the reverse shell executable dropped on the server?

The name of this file can be seen in the above picture.

Answer: docker

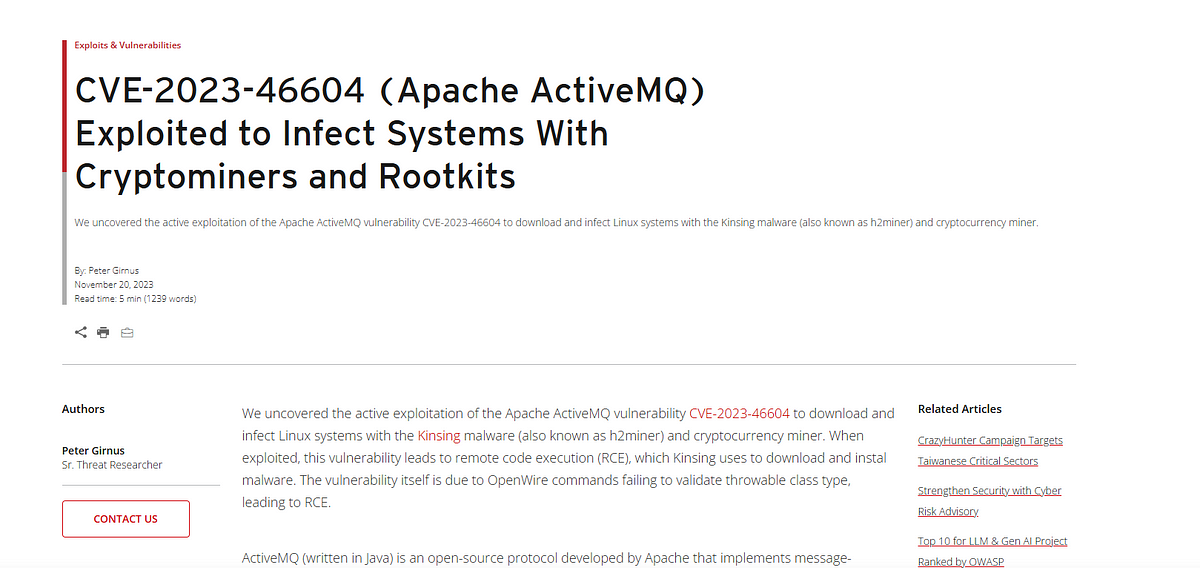
6. What Java class was invoked by the XML file to run the exploit?



ProcessBuilder is a Java class used to run system processes. From the above code it is clear that this is the class that the attacker is using to run the malicious script.

Answer: java.lang.ProcessBuilder

7. To better understand the specific security flaw exploited, can you identify the CVE identifier associated with this vulnerability?

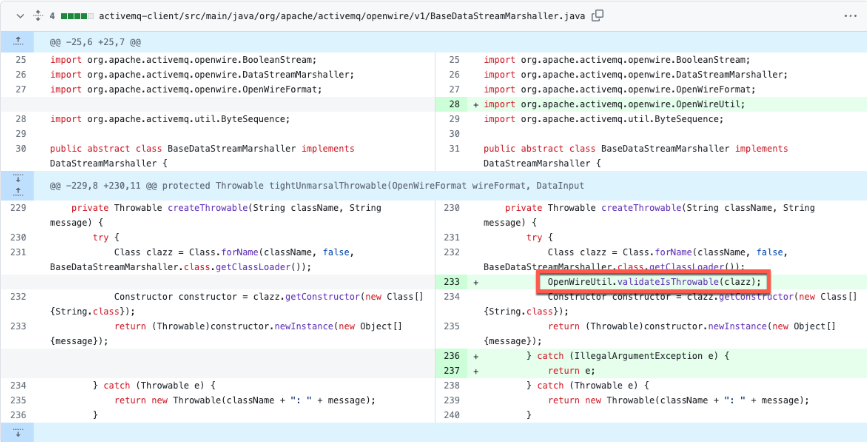


A quick google search gave an article from Trend Micro which exactly explains the same vulnerable behavior we observed in this traffic.

Answer: CVE-2023–46604

8. The vendor addressed the vulnerability by adding a validation step to ensure that only valid Throwable classes can be instantiated, preventing exploitation. In which **Java class** and **method** was this validation step added?

In the same article we can see the exact changes made in the patch that was released to mitigate this vulnerability.



The above snippet shows the exact validation step added in the code to mitigate the vulnerability.

Answer: BaseDataStreamMarshaller.createThrowable

This is the end of this walkthrough.