Official Incident Report

Event ID: 217

Rule Name: SOC254 - Apache OFBiz Auth Bypass and Code Injection 0-Day (CVE-2023-51467)

Table of contents

Official Incident Report **1**

Event ID: 217 1

Rule Name: SOC254 - Apache OFBiz Auth Bypass and Code Injection 0-Day (CVE-2023-51467) 1

Table of contents **2**

Alert **3**

Detection **4**

Verify 4

Collect Data 5

Analysis **8**

Examine The Traffic 11

Containment **17**

Summary **18**

Lesson Learned **19**

Remediation Actions **19**

Appendix **20**

MITRE ATT&CK 20

Artifacts 21

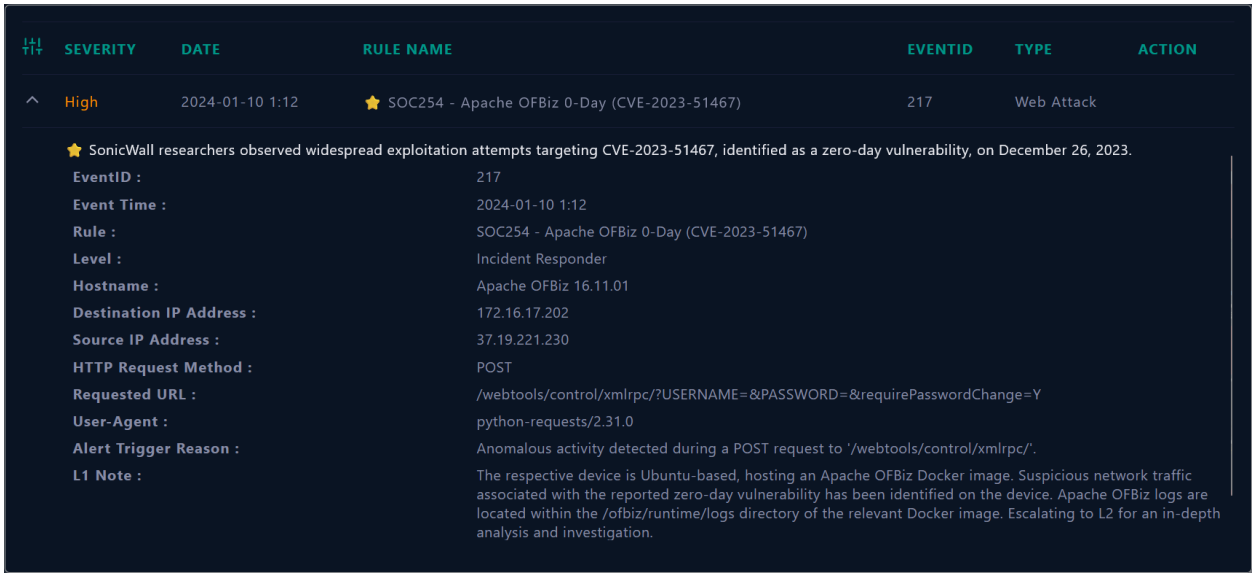
Alert

Based on the information that the alert provided, it appears that there is a suspicious Web Attack detected on a server named "**Apache OFBiz 16.11.01**" with an IP address of **172.16.17.202**. The Alert is triggered by the **SOC254** rule for **Apache OFBiz Auth Bypass and Code Injection 0-Day (CVE-2023-51467)**.

> **CVE-2023-51467** *vulnerability allows attackers to bypass authentication processes, granting them the ability to remotely execute arbitrary code. The SonicWall threat research team identified this authentication bypass vulnerability during the Root Cause Analysis (RCA) of the previously disclosed CVE-2023-49070 vulnerability.*

https://blog.sonicwall.com/en-us/2023/12/sonicwall-discovers-critical-apache-ofbiz-zero-day-authbiz/

The device action is marked as "Allowed", indicating that no action was taken by the device to prevent or block the related activities.



The Apache OFBiz server with version 16.11.01 received a POST request from the IP address 37.19.221[.]230. The request was made to the URL '/webtools/control/xmlrpc/' and had no specified username or password. The user agent used for this request was python-requests/2.31.0. This activity was flagged as anomalous, leading to the triggering of an alert.

Based on the provided trigger reason, suspicious activity for CVE-2023-51467 has been detected during a post request on the **Apache OFBiz 16.11.01** which could lead to unauthorized access or manipulation of data.

Detection

Verify

As the playbook suggests we can start investigating the alert by understanding why the alert was triggered

Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.

- The above instructions indicate that there has been a flagged anomalous activity involving suspicious activity for CVE-2023-51467 during a post request on the Apache OFBiz 16.11.01. This activity could potentially result in unauthorized access or manipulation of data. By understanding the rule name, it will be possible to determine the nature of the attack being faced.

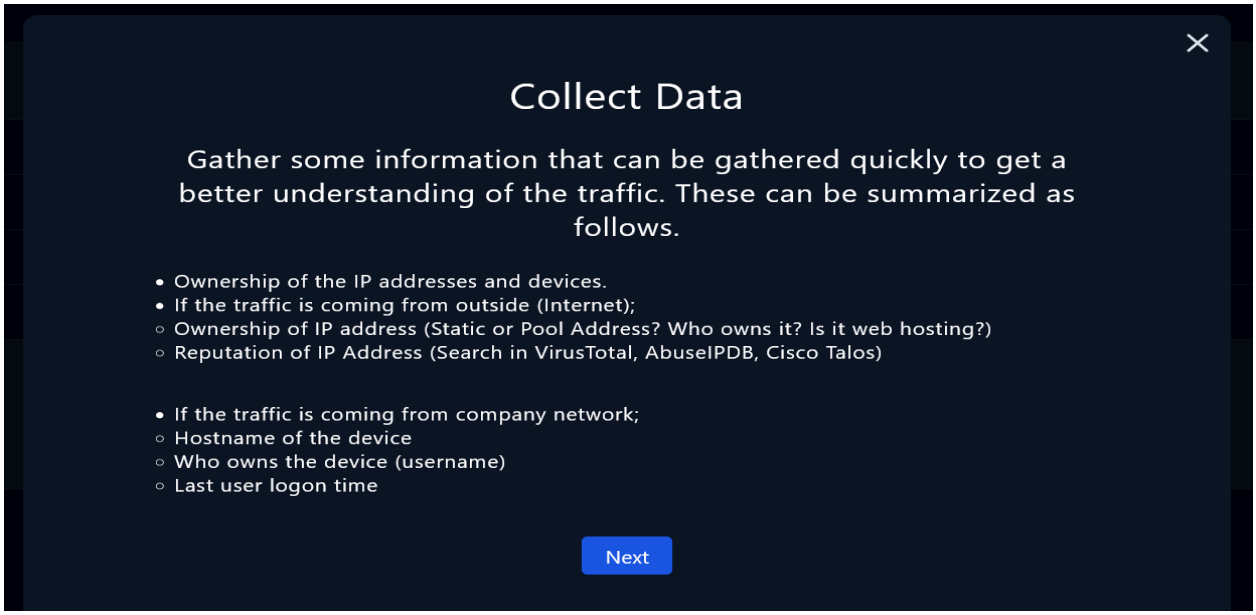
Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

The alert details provide information about the source and destination IP addresses involved in the suspicious network traffic:

- Source IP Address: 37.19.221[.]230
- Destination IP Address (Hostname): 172.16.17.202 (Apache OFBiz 16.11.01)

Collect Data

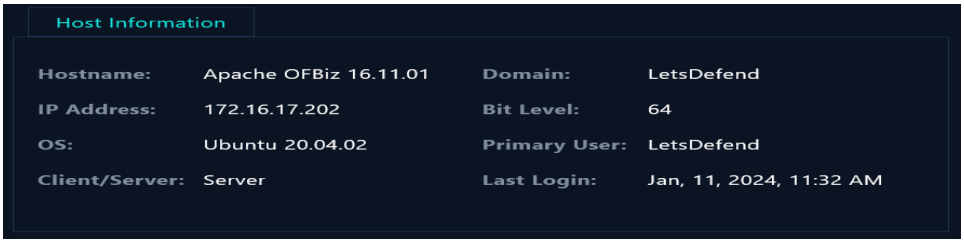
The next step in the playbook leads us to collect data and gather information about the relevant IP address.



Examining whether the IP address or domain has been linked to prior malicious activities and ownership of the IP address can provide insights into the current activity.

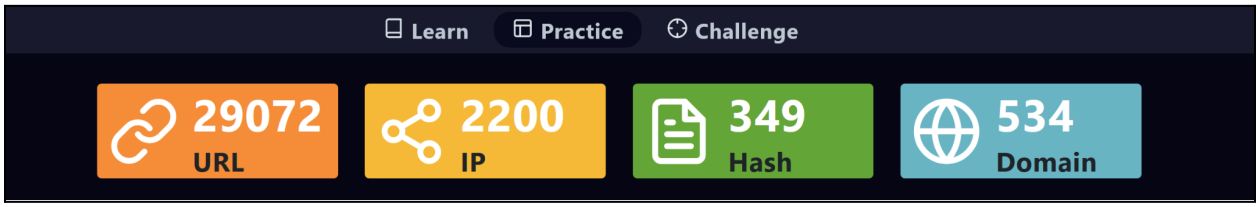
Hostname:	Apache OFBiz 16.11.01
IP Address:	172.16.17.202
Version:	OFBiz 16.11.01
Last Logon:	Jan, 11, 2024, 11:32 AM

When going through the technical details in SonicWall's article to check the affected versions, it's noted that Apache OFBiz 16.11.01 with the IP address 172.16.17.202 is affected by this vulnerability.



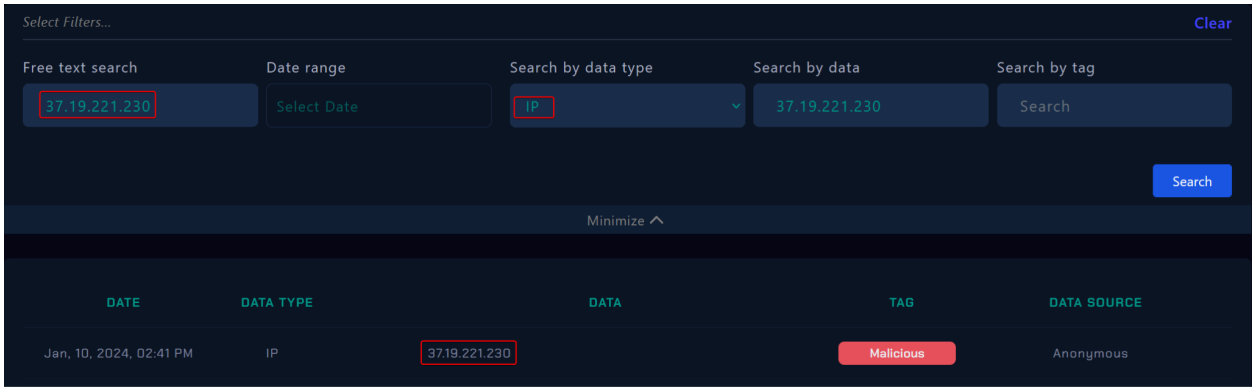
We can check if the traffic is inbound or outbound from the log management system by filtering the IP address of the host. As seen in the log management traffic is inbound.

On the LetsDefend threat intel tab, you'll find a comprehensive database dedicated to cataloging maliciously used information, such as IP addresses, domains, and other indicators of compromise.



https://app.letsdefend.io/threath-intelligence-feed

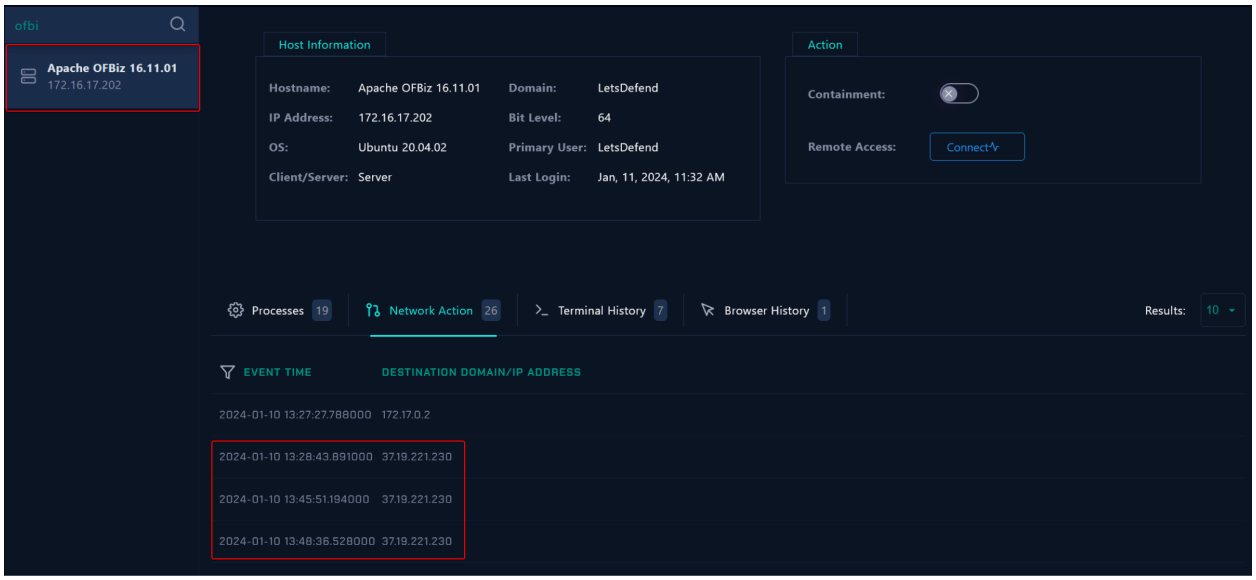
Upon cross-referencing the destination IP address discovered in the log management system with the Threat Intel tab, it was determined that the address has been categorized as malicious in nature.



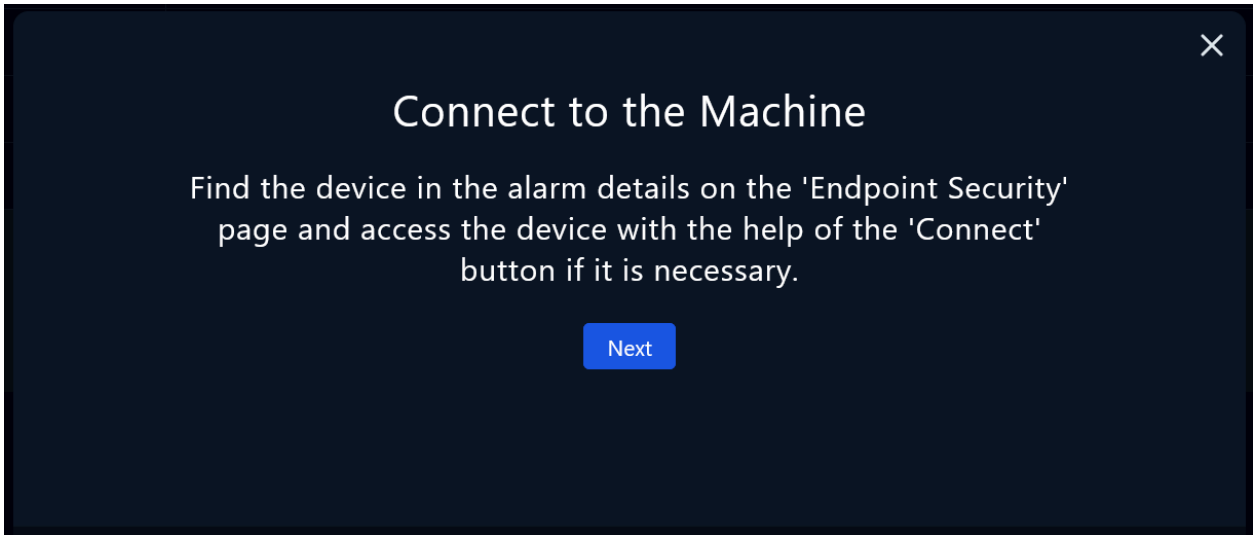
By cross-referencing the IP address with threat intelligence platforms such as Abuseip or Virustotal, we discovered that the IP address is malicious and reported many times.

Based on the information provided by VirusTotal, the IP address has been flagged as malicious by **2** antivirus engines. Additionally, in the community tab, it is seen that this IP is contained in a collection.

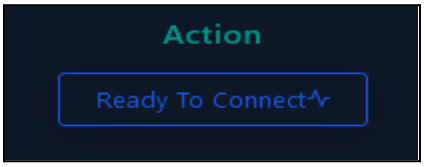
The IOC also seen in the network actions of the host machine.



Analysis



We can proceed with connecting to the host machine for further analysis. This can easily be done from the Endpoint Security tab by searching for the hostname or IP address and clicking the "Connect" button.



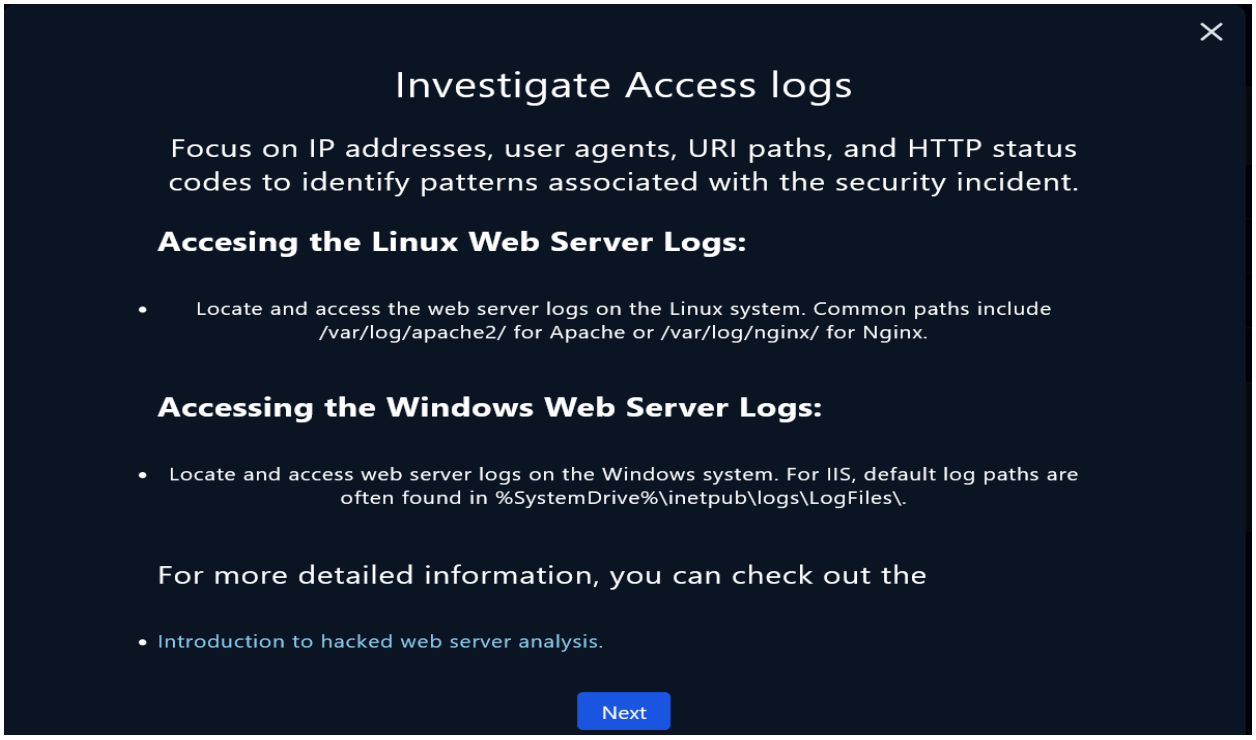
After connecting we can check if the docker is still up. Running this command will allow us to determine the status of the docker.

>docker ps -a

```
root@ip-172-31-17-104:~# docker ps
CONTAINER ID   IMAGE                          COMMAND                  CREATED      STATUS          PORTS
                                                                       NAMES
1e4d7de50ed5   marcopinball/ofbiz-demo:latest   "/bin/sh -c './gradl…"   9 days ago   Up 15 minutes   0.0.0.0:808
0->8080/tcp, :::8080->8080/tcp, 0.0.0.0:8443->8443/tcp, :::8443->8443/tcp   pedantic_elgamal
```

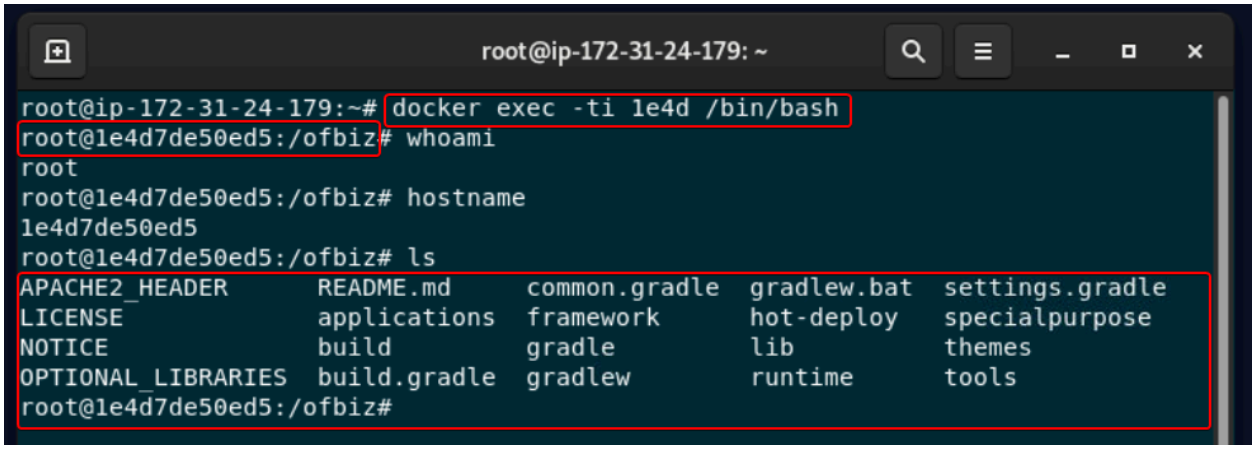
We have identified that the docker is still active and running on the host machine.

The next step is Investigating the access logs. Focusing on IP addresses, user-agents, paths, HTTP status codes and timestamps will help us identify any suspicious or malicious activity.

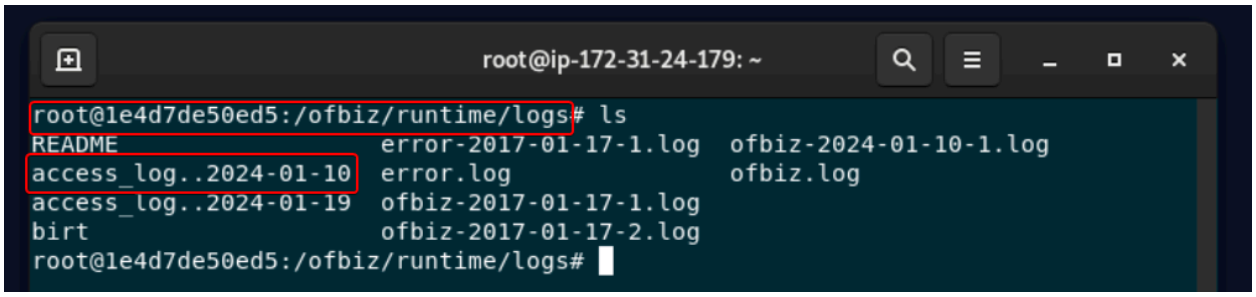


By analyzing these logs, we can gain insights into potential vulnerabilities or security breaches. Additionally, cross-referencing the information with known threat intelligence sources can provide us with a better understanding of the nature and severity of any identified threats.

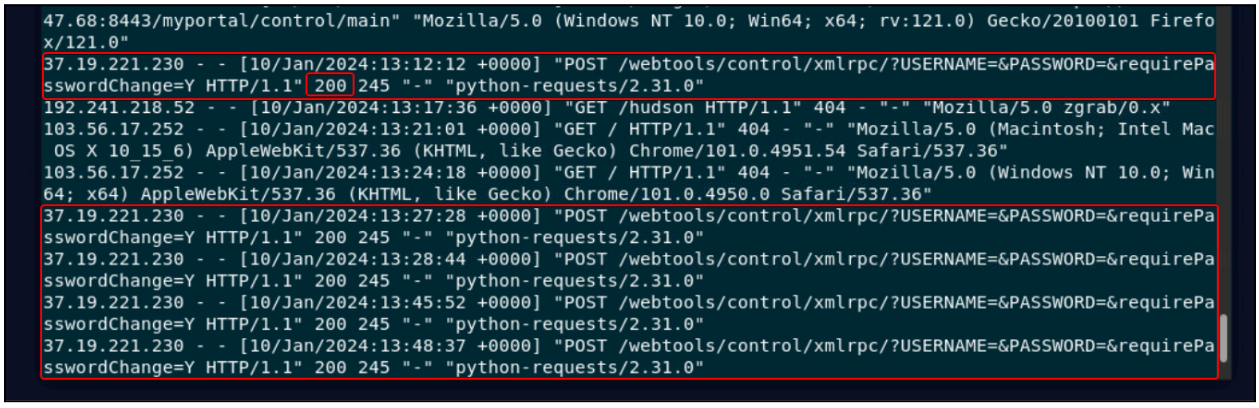
Since the Apache OFBiz running on a docker image we need to gain a shell on the related docker image. To do that we can run the given command:



This analysis can be conducted by examining the logs located within the /ofbiz/runtime/logs directory of the docker image. The directory in question contains the Apache access log for the date when the alarm was triggered.



Upon analyzing the content of the relevant log, it was observed that there are multiple suspicious requests as detailed in the alarm, all originating from the same IP address.

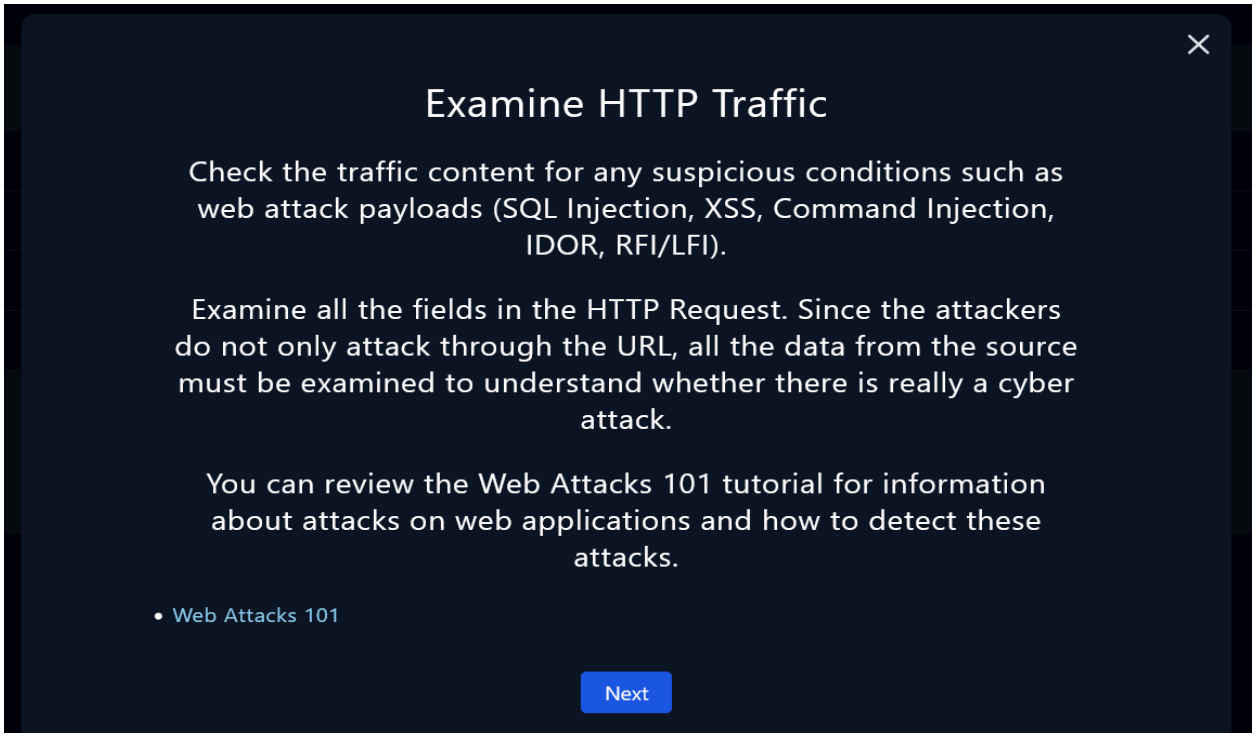


- **IP Address:** 37.19.221.230
- **Date and Time:** 10/Jan/2024:13:12:12 +0000
- **HTTP Method:** POST
- **Requested URL:** /webtools/control/xmlrpc/?USERNAME=&PASSWORD=&requirePasswordChange=Y
- **HTTP Protocol:** HTTP/1.1
- **HTTP Status Code:** 200
- **Bytes Sent:** 245
- **Referrer:** "-"
- **User-Agent:** "python-requests/2.31.0"

This log entry indicates a POST request to the specified URL from the IP address 37.19.221.230, using the user-agent "python-requests/2.31.0", and it received a successful HTTP status code 200 with 245 bytes sent.

Examine The Traffic

The third step of the playbook involves examining the traffic.This step is crucial in identifying any suspicious or malicious activities and understanding the overall network behavior. Additionally, examining the traffic can provide valuable information for further investigation and potential security enhancements.



Before examining HTTP traffic, it is crucial to investigate the payloads used in exploiting the relevant vulnerability. The items mentioned in the details of SonicWall's Apache OFBiz security report will facilitate the analysis of the incident.

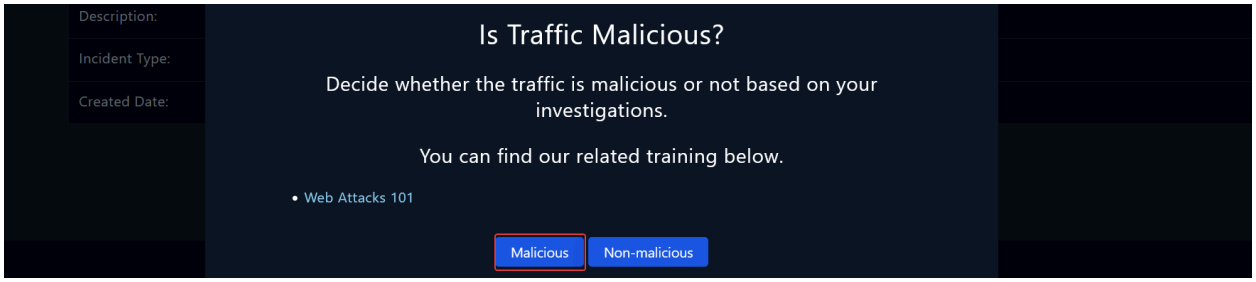
Testcase 1

Our first test case was based on using empty *USERNAME* and *PASSWORD* parameters while including the parameter *requirePasswordChange=Y* in URI This test was derived from the testing of CVE-2023-49070 during our signature development to ensure detection in all use cases. The question was posed, what if there is no username and password in the request? For instance, the request might look like https[:]//www.example.com:8443/webtools/control/xmlrpc/?USERNAME=&PASSWORD=&requirePasswordChange=Y.

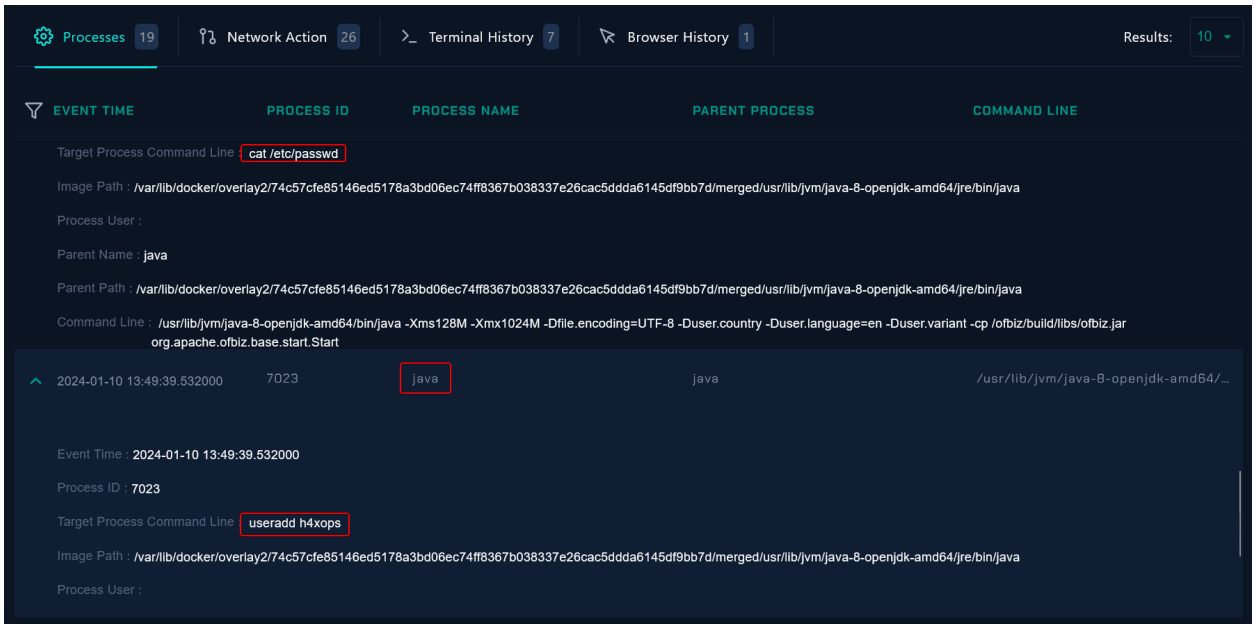
Considering that this attack involves a 0-day exploit targeting the Apache OFBiz 16.11.01, we can use the time when the alert was triggered as a reference point for analysis. Filtering the Apache OFBiz 16.11.01 IP address in log management allows us to view the logs.

Firewall logs for the date of January 10th are available. These logs are essential for monitoring and analyzing network traffic and security events on that specific date.

As seen in the raw log source process for the traffic is Java and the firewall action is success.



We have observed that the traffic originates from a Java process. Let's proceed to Endpoint Security and analyze the processes. In Endpoint Security, we will identify the specific Java process that is generating the traffic. This will allow us to examine the process's behavior and determine if it is behaving maliciously or if it has been compromised. By analyzing the processes, we can gather more information about the incident and make informed decisions on how to mitigate the threat.

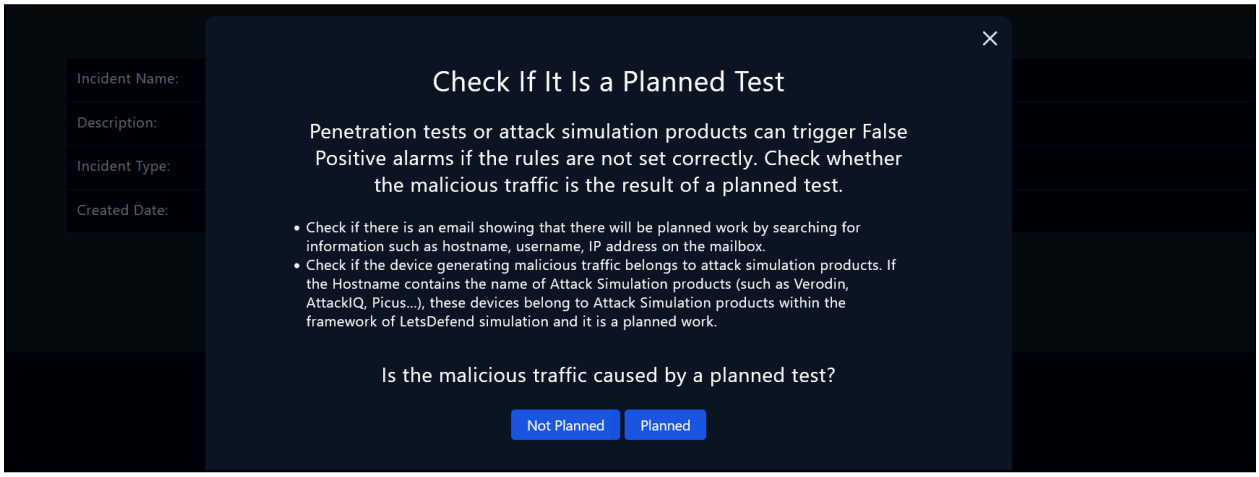


The attacker executed malicious code on the host by sending malicious POST requests.

Based on our analysis, we have confirmed that the traffic is **malicious.**

The next playbook step requires us to find the attack type. The analysis confirms that the relevant attack type is Apache OFBiz Auth Bypass and Code Injection 0-Day (CVE-2023-51467). The answer for the attack type is Other.

When examining the relevant web traffic, it has been observed that the IP address associated with the attacker is listed as an Indicator of Compromise (IOC) in global resources. Furthermore, no evidence suggesting that the respective attack was conducted for testing purposes has been identified in email records or any other section of the investigation.



The IP and hostname information of the relevant hostname were searched within the emails received during the specified dates. However, no evidence related to a planned activity has been observed through this investigation.
The answer for this step is “Not Planned”

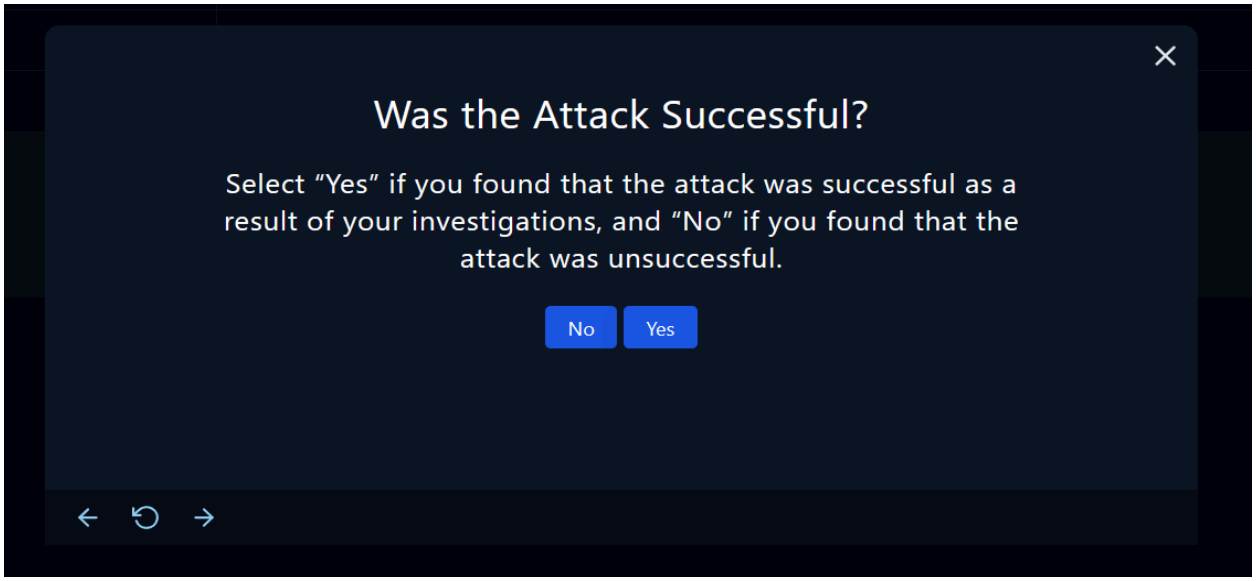
The Next step of the playbook involves examining the direction of the traffic.

To determine the direction of traffic, we will review the all logs we gathered from our security products on the log management page. The alert creation time will be a key reference for us to investigate the incident.

In the log management page, all of the malicious traffic is from the Internet -> Company Network.

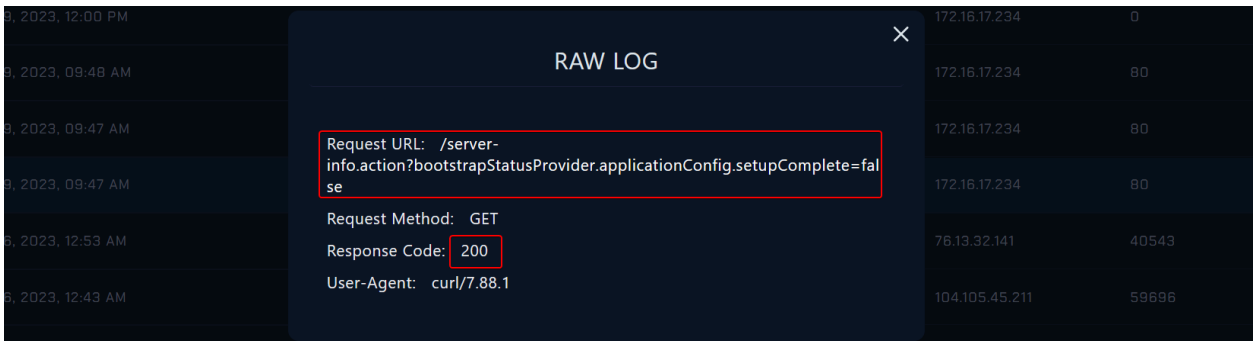
The source address is 37.19.221[.]230 and the destination address is 172.16.17.202. So the answer for this playbook step is Internet -> Company Network.

The next step in the playbook is to assess whether the attack was successful. This involves analyzing the impact of the attacker's actions and determining if they were able to achieve their objectives.



Analyzing the responses enables us to ascertain whether a malicious implant has been detected on the system, thus providing insights into the system's security compromised status.

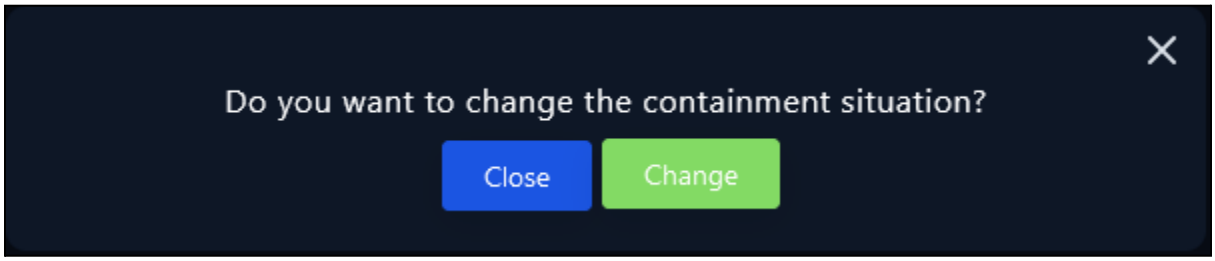
Let's filter the IP address of the machine (172.16.17.202) that initiated these requests on the log management system.



Based on the HTTP response code of 200, it appears that the request to /server-info.action?bootstrapStatusProvider.applicationConfig.setupComplete=false was successful. Through log analysis, we have confirmed that **the attack was successful**.

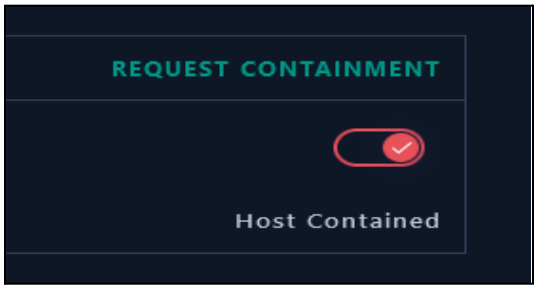
Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Isolation of the host can be made from the endpoint security tab.

Hostname	Apache OFBiz 16.11.01
IP Address	172.16.17.202



After the containment, we can close the alert from the investigation channel.

Summary

The alert report details the detection of suspicious web attack on the Apache OFBiz 16.11.01 (IP: 172.16.17.202) triggered by the SOC235 - Atlassian Apache OFBiz Broken Access Control 0-Day CVE-2023-51467). This vulnerability allows threat actors to gain unauthorized access to sensitive information and perform malicious activities on the affected server.

Upon analysis, it's found that the device action was marked as "allowed," meaning no action was taken to prevent or block the execution of the web attack. The source IP, 37.19.221[.]230, used the user agent "python-requests/2.31.0" to potentially exploit CVE-2023-51467. The investigation, following a detailed playbook, cross-referenced the IP, linking it to malicious activity through threat intelligence platforms like Let's Defend and VirusTotal. SonicWall's report further flagged the IP as Command and Control (C2) and malicious.

Analyzing traffic logs revealed a successful attack pattern, exploiting Apache OFBiz vulnerabilities. Despite an exhaustive examination, no evidence of a planned activity was found in email records. The playbook's final step confirmed the attack's success, as the HTTP response code 200 indicated the completion of the malicious request.

Containment measures are recommended due to the high likelihood of system compromise. Finally, the alert is closed after a thorough investigation, and appropriate actions are taken to mitigate the threat.

Lesson Learned

- Timely threat intelligence is crucial for identifying and responding to emerging vulnerabilities and exploits.

- Monitoring for specific indicators of compromise (IOCs) helps detect potential security threats, but they should be supplemented with in-depth analysis.

- Effective threat hunting and detailed investigation are essential to understand the scope of an attack and its potential impact on the organization.

- Staying informed about vulnerabilities and applying patches or mitigations is vital for system security.

- Enabling and collecting logs from various operating systems can significantly enhance visibility into your network's security posture.

Remediation Actions

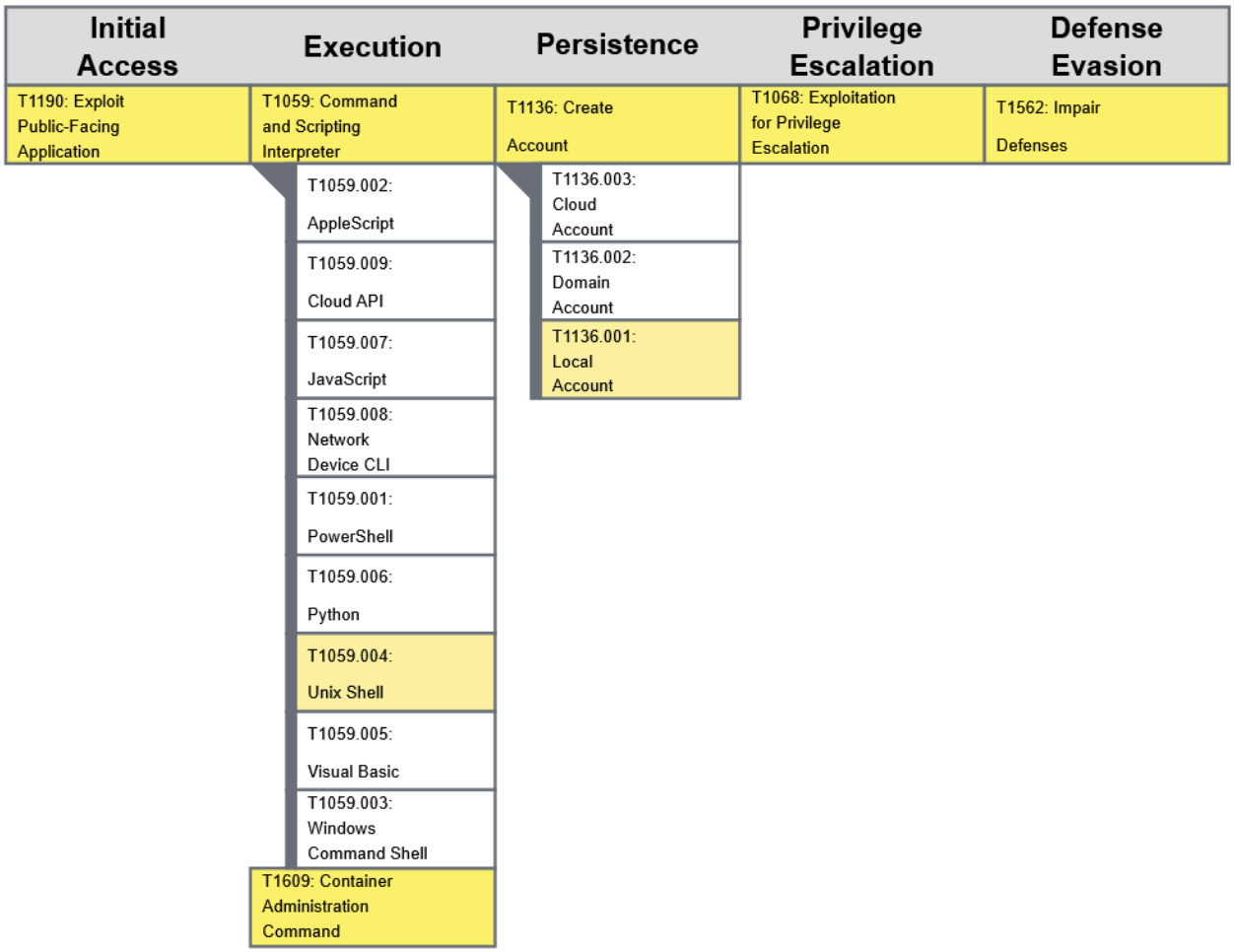
- Apply security patches or updates to address the CVE-2023-51467 vulnerability in the Apache OFBiz 16.11.01 to eliminate the attack vector.

- Restrict external network access to Apache OFBiz 16.11.01 and Server instances accessible via the public internet, until the necessary upgrades can be performed

- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.

Appendix

MITRE ATT&CK



MITRE Tactics	MITRE Techniques
Initial Access	T1190: Exploit Public-Facing Application
Execution	T1059: Command and Scripting Interpreter
Execution	T1609: Container Administration Command
Persistence	T1136: Create Account
Privilege Escalation	T1068: Exploitation for Privilege Escalation
Impact	T1562: Impair Defenses

Artifacts

IOC TYPE	VALUE
IPv4	37.19.221[.]230
URI	/xmlrpc/?USERNAME=&PASSWORD=&requirePasswordChange=Y