Homework 5: Incident Response

Incident Summary

Incident Name: Cisco IOS XE Unauthenticated Remote Code Execution

Incident Date: 10/18/2023

Incident Analyst: Shikha Mehta

Incident Analyst UID: 120222382

Incident Analyst Section: ENPM685 0301

Time Spent Analyzing Incident: 6 hours

Incident Summary:

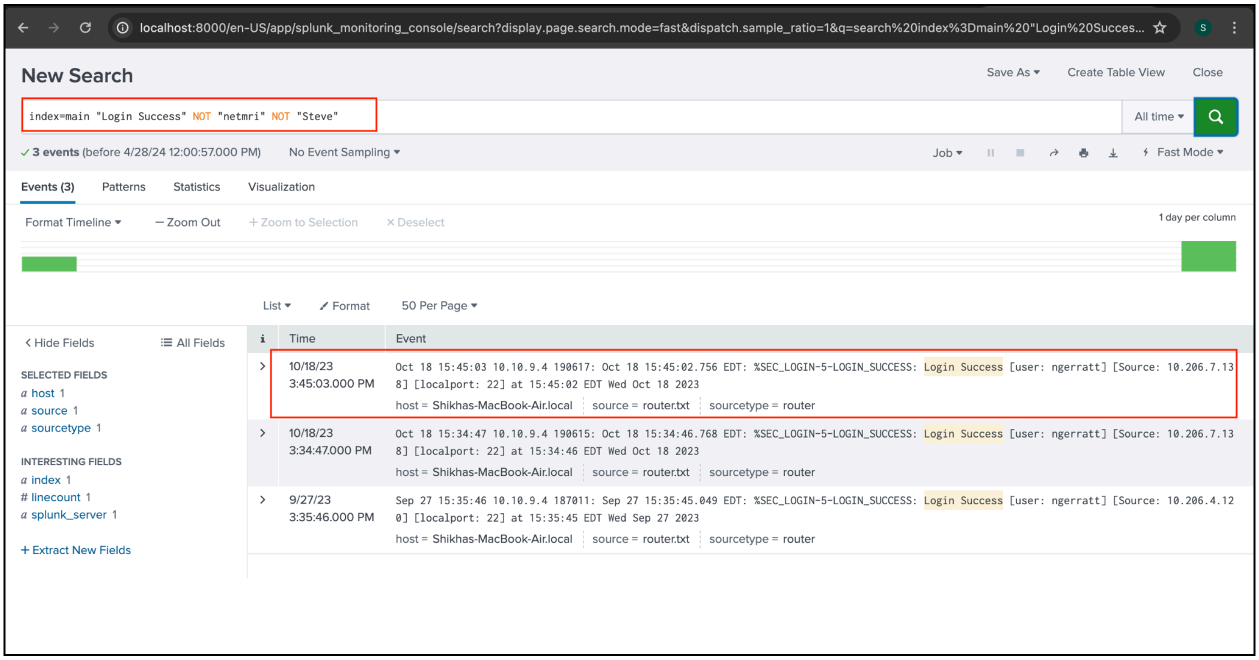
On October 18, 2023, a vulnerability in the web UI feature of Cisco IOS XE Software allowed an authenticated, remote attacker to inject commands with the highest privilege level of admin that gives the user full control over the router. It was later discovered that the Cisco IOS XE router was compromised by the CVE-2023-20198 vulnerability since it had its web user interface exposed to the public.

Two clusters of vulnerabilities were exploited by the threat actors: in the first cluster, the actors tested their code in September, and in the October activity, they expanded their operation to include implant deployment for persistent access. After the incident, vendor instructions were immediately followed to determine if the affected router was exposed to the public and positive findings were immediately reported to the CISA.

Incident Notes:

DETECT: How was the incident detected?

On October 18, when a customer's device displayed suspicious activity, malicious activity was discovered. There is proof that an unknown and suspicious IP address created a new user account (ngerratt).



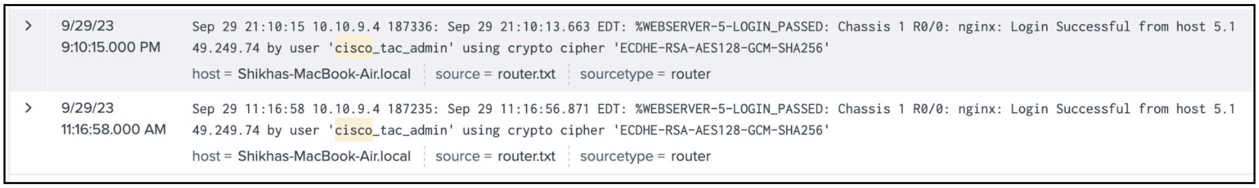
```
index=main "Login Success" NOT "netmri" NOT "Steve"
```

✓ 3 events (before 4/28/24 12:00:57.000 PM)

Time	Event
10/18/23 3:45:03.000 PM	Oct 18 15:45:03 10.10.9.4 190617: Oct 18 15:45:02.756 EDT: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ngerratt] [Source: 10.206.7.138] [localport: 22] at 15:45:02 EDT Wed Oct 18 2023 host = Shikhas-MacBook-Air.local source = router.txt sourcetype = router
10/18/23 3:34:47.000 PM	Oct 18 15:34:47 10.10.9.4 190615: Oct 18 15:34:46.768 EDT: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ngerratt] [Source: 10.206.7.138] [localport: 22] at 15:34:46 EDT Wed Oct 18 2023 host = Shikhas-MacBook-Air.local source = router.txt sourcetype = router
9/27/23 3:35:46.000 PM	Sep 27 15:35:46 10.10.9.4 187011: Sep 27 15:35:45.049 EDT: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ngerratt] [Source: 10.206.4.120] [localport: 22] at 15:35:45 EDT Wed Sep 27 2023 host = Shikhas-MacBook-Air.local source = router.txt sourcetype = router

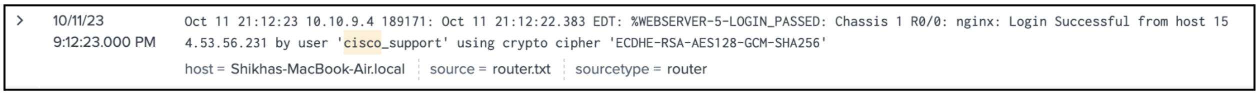
ANALYSIS: What triage and analysis was performed?

Further investigation revealed that the activity in question began on September 29, when a legitimate user from a suspicious IP address created a local user account with the name "cisco_tac_admin." **Search command: index=main “cisco”**



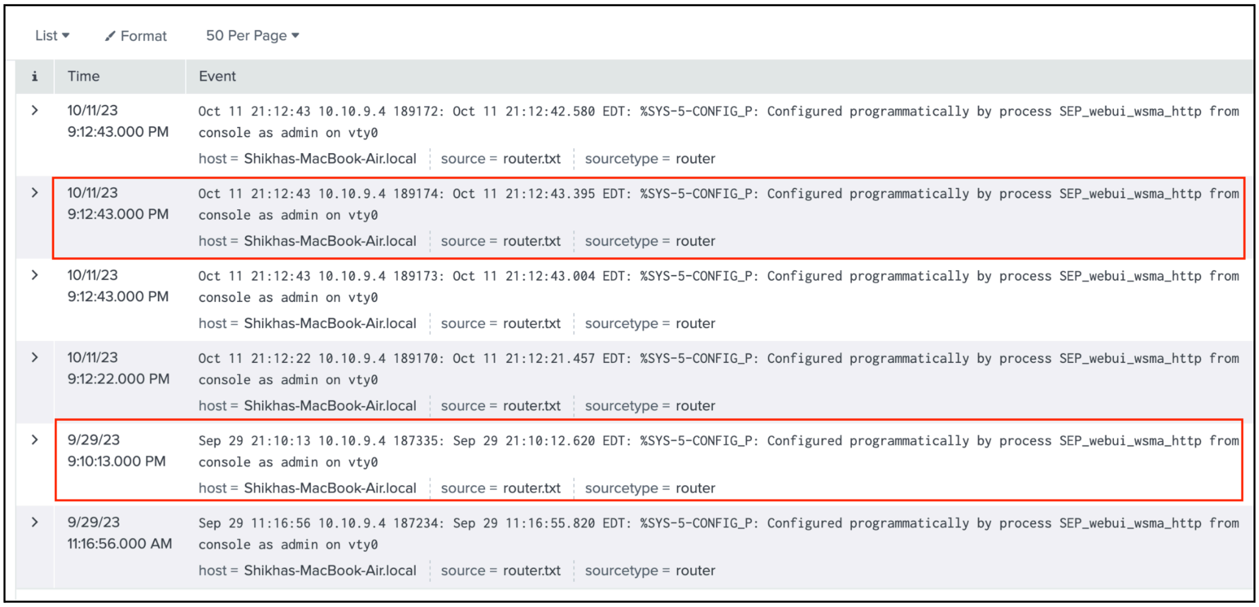
9/29/23 9:10:15.000 PM	Sep 29 21:10:15 10.10.9.4 187336: Sep 29 21:10:13.663 EDT: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host 5.149.249.74 by user 'cisco_tac_admin' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256' host = Shikhas-MacBook-Air.local source = router.txt sourcetype = router
9/29/23 11:16:58.000 AM	Sep 29 11:16:58 10.10.9.4 187235: Sep 29 11:16:56.871 EDT: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host 5.149.249.74 by user 'cisco_tac_admin' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256' host = Shikhas-MacBook-Air.local source = router.txt sourcetype = router

When a different suspicious IP address was used by an unauthorized user to create an account under the name "cisco_support," another cluster of suspicious activity was discovered by October 11.



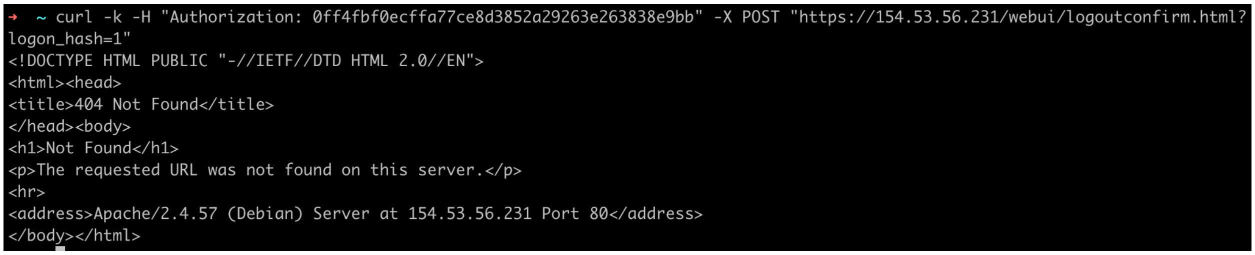
```
>  10/11/23          Oct 11 21:12:23 10.10.9.4 189171: Oct 11 21:12:22.383 EDT: %WEBSERVER-5-LOGIN_PASSED: Chassis 1 R0/0: nginx: Login Successful from host 15
   9:12:23.000 PM    4.53.56.231 by user 'cisco_support' using crypto cipher 'ECDHE-RSA-AES128-GCM-SHA256'
                     host = Shikhas-MacBook-Air.local | source = router.txt | sourcetype = router
```

An implant with a configuration file was deployed as part of the October activity. The implant was programmatically configured by running SEP_webui_wsma_http as admin from the console.



```
i  Time              Event
>  10/11/23          Oct 11 21:12:43 10.10.9.4 189172: Oct 11 21:12:42.580 EDT: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from
   9:12:43.000 PM    console as admin on vty0
                     host = Shikhas-MacBook-Air.local | source = router.txt | sourcetype = router
>  10/11/23          Oct 11 21:12:43 10.10.9.4 189174: Oct 11 21:12:43.395 EDT: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from
   9:12:43.000 PM    console as admin on vty0
                     host = Shikhas-MacBook-Air.local | source = router.txt | sourcetype = router
>  10/11/23          Oct 11 21:12:43 10.10.9.4 189173: Oct 11 21:12:43.004 EDT: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from
   9:12:43.000 PM    console as admin on vty0
                     host = Shikhas-MacBook-Air.local | source = router.txt | sourcetype = router
>  10/11/23          Oct 11 21:12:22 10.10.9.4 189170: Oct 11 21:12:21.457 EDT: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from
   9:12:22.000 PM    console as admin on vty0
                     host = Shikhas-MacBook-Air.local | source = router.txt | sourcetype = router
>  9/29/23           Sep 29 21:10:13 10.10.9.4 187335: Sep 29 21:10:12.620 EDT: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from
   9:10:13.000 PM    console as admin on vty0
                     host = Shikhas-MacBook-Air.local | source = router.txt | sourcetype = router
>  9/29/23           Sep 29 11:16:56 10.10.9.4 187234: Sep 29 11:16:55.820 EDT: %SYS-5-CONFIG_P: Configured programmatically by process SEP_webui_wsma_http from
   11:16:56.000 AM   console as admin on vty0
                     host = Shikhas-MacBook-Air.local | source = router.txt | sourcetype = router
```

This curl command executed a request to the device’s Web UI to see if the implant is present. It returned a 404 HTTP response with an HTML page consisting of a “404 Not Found” message, that means a known one of the first two known variants of the implant was present. However, the implant is no longer active i.e. it is a non-persistent implant.



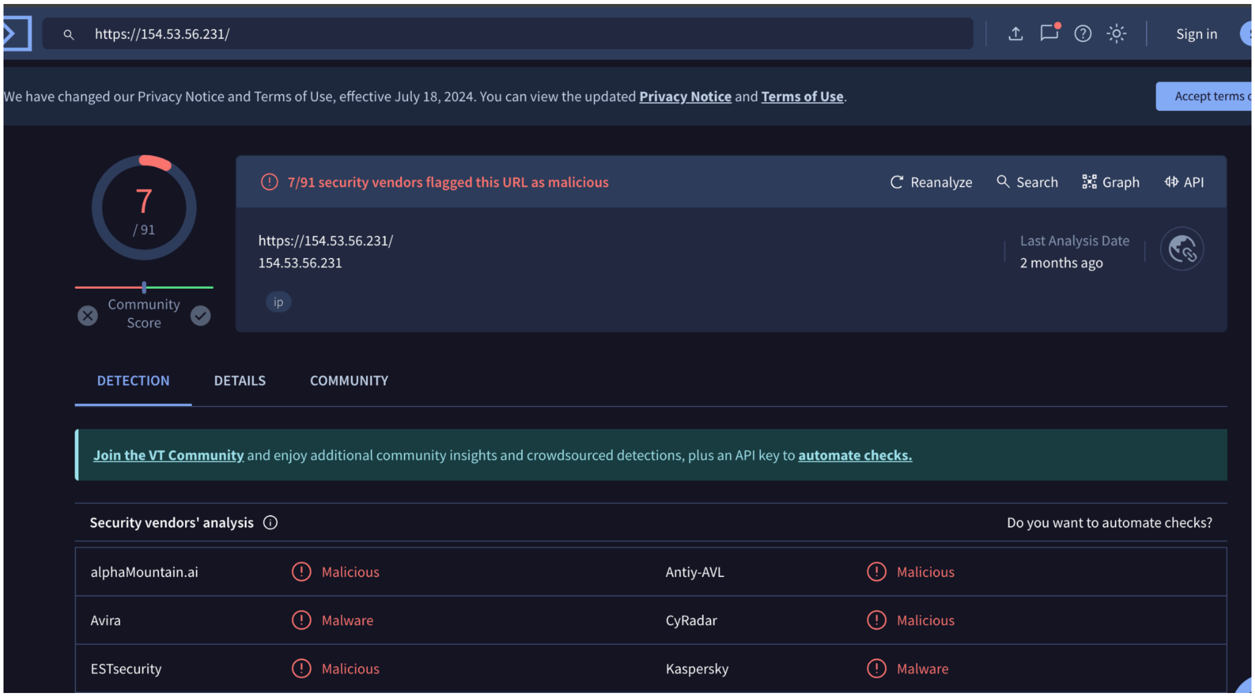
```
➜  ~ curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X POST "https://154.53.56.231/webui/logoutconfirm.html?
logon_hash=1"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.57 (Debian) Server at 154.53.56.231 Port 80</address>
</body></html>
```

ANALYSIS: What Indicators of Compromise were discovered?

Attacker IP: 154.53.56.231

C2: https://154.53.56.231/

VirusTotal page for this IP address:



We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated **Privacy Notice** and **Terms of Use**.

7/91 security vendors flagged this URL as malicious

https://154.53.56.231/
154.53.56.231

Last Analysis Date
2 months ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis ⓘ

Do you want to automate checks?

alphaMountain.ai	ⓘ Malicious	Antiy-AVL	ⓘ Malicious
Avira	ⓘ Malware	CyRadar	ⓘ Malicious
ESTsecurity	ⓘ Malicious	Kaspersky	ⓘ Malware

Analysis report:

https://www.joesandbox.com/analysis/1345836/0/html

CONTAIN: What containment and/or eradication steps were performed?

To eliminate the attack vector for these vulnerabilities, the HTTP Server feature was disabled. This was done by using the “no ip http server” or “no ip http secure-server” command in global configuration mode. Limiting access to the HTTP Server to trusted networks limits exposure to these vulnerabilities.

RECOVERY: What recovery steps were taken?

All the affected devices were upgraded and proper access control mechanisms were implemented. Also, network traffic and system logs were continuously monitored for signs of compromise.

POST INCIDENT ACTIVITY: Lessons Learned / Follow up items

-Identify gaps in security measures, understand the attack vectors, and improve incident response procedures.

-Implement regular vulnerability assessments, security awareness training, and access controls to prevent similar incidents in the future.

-Develop incident response plans, including escalation procedures, to enhance preparedness for future incidents.