LetsDefend

Official incident report

Event ID: 193

Rule Name: SOC231 - Cisco IOS XE Web UI ZeroDay (CVE-2023-20198)

Made By

LinkedIn: Engineer.Ahmed Mansour

Link: https://www.linkedin.com/in/ahmed-mansour-5631b5323/

Github link: https://github.com/AhmedMansour93

Table of contents

Event Details

Event ID:
193

Event Date and Time:
Oct, 20, 2023, 12:35 PM

Rule:
SOC231 - Cisco IOS XE Web UI ZeroDay (CVE-2023-20198)

Level:
Incident Responder

Hostname:
Cisco Catalyst 8000V

HTTP Request Method:
POST

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 mail group (soc@letsdefend.io) 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.

Network Information Details

Destination IP Address:
172.16.20.59 internal

Source IP Address:
185.177.124.100 external

Destination IP Address:

- **172.16.17.101 (Internal)**
  This is an internal IP address associated with a device within your network. IP addresses in the range 172.16.0.0 to 172.31.255.255 are private and used for internal networks. These addresses are not routable on the public internet, meaning they belong to your organization's internal infrastructure.

Source IP Address:

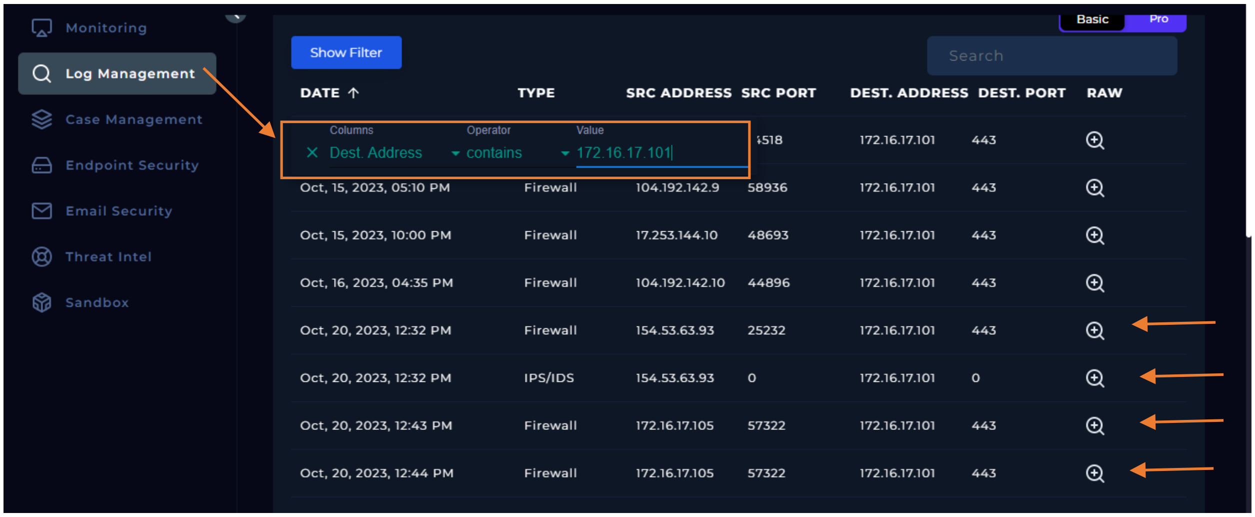
- **154.53.63.93 (External)**
  This is a public IP address, meaning it originates from outside your organization's internal network. It indicates that the attack came from an external source, likely over the internet.
  The attack is external.

Analysis:

Log Management

We'll proceed by entering the destination IP address and reviewing the results. Based on the time and date of the attack.

Please refer to the attached image for further details regarding the attack.



Columns: Dest. Address
Operator: contains
Value: 172.16.17.101

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
			:518	172.16.17.101	443	⊕
Oct, 15, 2023, 05:10 PM	Firewall	104.192.142.9	58936	172.16.17.101	443	⊕
Oct, 15, 2023, 10:00 PM	Firewall	17.253.144.10	48693	172.16.17.101	443	⊕
Oct, 16, 2023, 04:35 PM	Firewall	104.192.142.10	44896	172.16.17.101	443	⊕
Oct, 20, 2023, 12:32 PM	Firewall	154.53.63.93	25232	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, 12:43 PM	Firewall	172.16.17.105	57322	172.16.17.101	443	⊕
Oct, 20, 2023, 12:44 PM	Firewall	172.16.17.105	57322	172.16.17.101	443	⊕

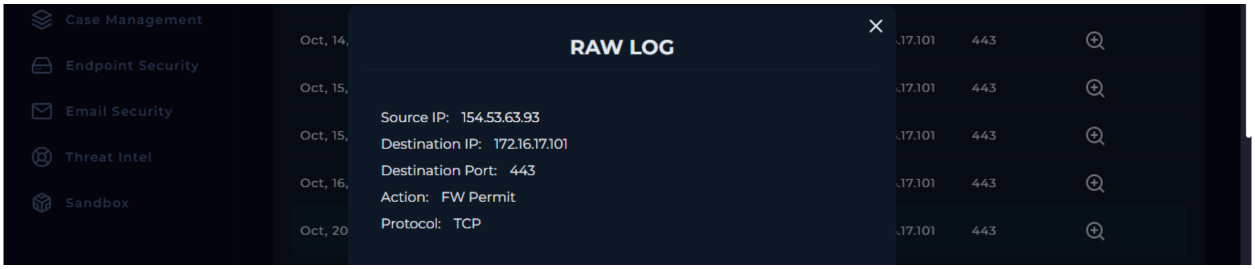
4 Logs records for the destination IP.

Please refer to the attached image for further details regarding the attack.

We will explain all of them step by step

Log Analysis

- **Log1:**



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

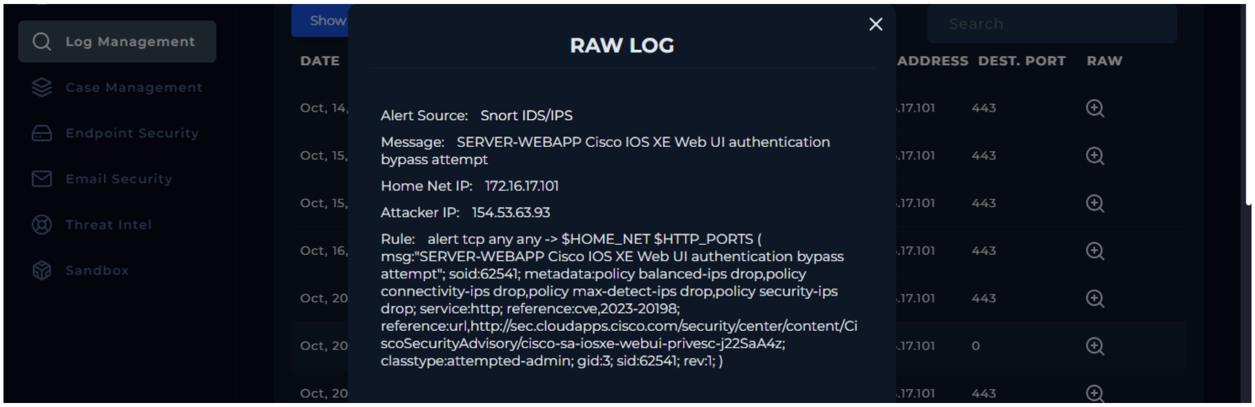
- **Explanation:**

The source IP (154.53.63.93) from an external network is attempting to communicate with an internal device (172.16.17.101) on port 443, which is used for HTTPS. The firewall allowed (FW Permit) this connection.
Port 443 indicates that the communication is encrypted, possibly targeting a web-based interface, which matches the characteristics of Cisco IOS XE Web UI (the vulnerability being discussed).

- **Interpretation:**

The attacker is trying to reach the web interface of the device at 172.16.17.101. This is the first step where an external IP attempts to access the internal device.

- **Log2:**



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/Ci
scoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z;
classtype:attempted-admin; gid:3; sid:62541; rev:1; )
```

- **Explanation:**

This Snort alert is triggered by an attempt to exploit **CVE-2023-20198**. The rule detected a suspicious attempt by IP 154.53.63.93 to bypass authentication on a web application running on 172.16.17.101. The rule is specifically written to catch attempts to exploit Cisco IOS XE Web UI's authentication bypass vulnerability.

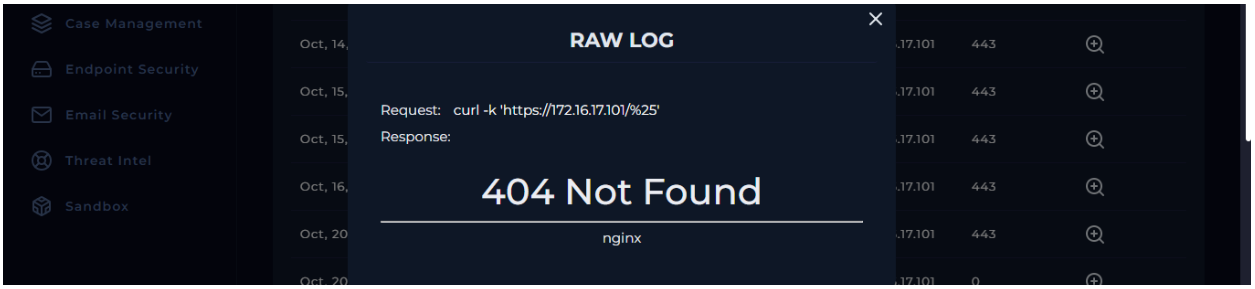
The details in the rule include:

- **Service:** HTTP (even though the initial log shows HTTPS, the actual requests may involve HTTP once inside the network).
- **CVE Reference:** CVE-2023-20198.
- **Action:** The rule identifies the activity as an "attempted-admin," meaning the attacker is likely trying to gain administrative control via a bypass method.

- **Interpretation:**

The attacker, from IP 154.53.63.93, is attempting to exploit a known vulnerability in the Cisco IOS XE Web UI (CVE-2023-20198) on the internal device 172.16.17.101. This Snort alert is a key indicator that a targeted attack is happening.

- **Log3:**



Request: curl -k 'https://172.16.17.101/%25'
Response:

404 Not Found

nginx

- **Explanation:**

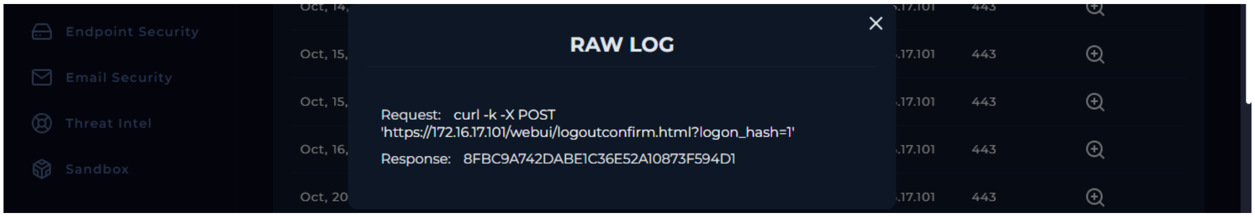
The attacker uses the `curl` command to make an HTTP request to the device. The URL they used contains `%25`, which represents a URL-encoded `%`, a typical attempt to exploit or manipulate URL parameters. This kind of request may be testing for potential weaknesses in input validation or trying to access certain protected resources by bypassing filters.

The response from the server is `404 Not Found`, meaning the requested resource (in this case, likely related to the Web UI) wasn't found, but the server did respond, which confirms that the request reached the device.

- **Interpretation:**

This `curl` request seems to be part of the attacker's effort to probe the system and look for vulnerabilities. They are testing various inputs to see how the device responds, likely in preparation for further exploitation. However, this specific request didn’t yield useful results for the attacker.

- **Log4:**



RAW LOG

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

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

- **Explanation:**
  The attacker sends a POST request to the `/webui/logoutconfirm.html` endpoint with a parameter `logon_hash=1`. This request might be part of an attempt to trick the Web UI into logging out or bypassing authentication in some way by manipulating session tokens or hashes. The response is a long alphanumeric string, likely a session or authentication token.
- **Interpretation:**
  This is a more advanced step in the attack. The attacker is likely trying to exploit the authentication bypass by either forging or tampering with session tokens. The response they received (`8FBC9A742DABE1C36E52A10873F594D1`) could indicate that the server accepted the request and generated or returned a token. This token may give the attacker access to authenticated sessions or allow them to bypass authentication checks.

Summary of Events:

1. **Initial Access (Log 1):**
   An external attacker (IP 154.53.63.93) initiates communication with an internal device (172.16.17.101) over HTTPS (port 443). The firewall permits this traffic, allowing the attacker to attempt interaction with the device.
2. **Exploitation Attempt Detected (Log 2):**
   A Snort IDS/IPS alert is triggered by an attempted exploitation of **CVE-2023-20198**, a vulnerability in Cisco IOS XE Web UI. This alert signals that the attacker is trying to bypass the web UI's authentication system, likely to gain unauthorized access to administrative functions.
3. **Probing for Weaknesses (Log 3):**
   The attacker uses a `curl` command to test potential weaknesses in URL parsing or input handling by sending a `%25` (encoded %) to the device's web interface. This particular attempt results in a 404 error, but it confirms that the server is responding and reachable.
4. **Authentication Bypass Attempt (Log 4):**
   The attacker makes a more sophisticated attempt to exploit the system by sending a POST request to the `/webui/logoutconfirm.html` endpoint, potentially manipulating session tokens to bypass authentication. The server responds with what appears to be a session token or a hashed value, suggesting that the attack may be progressing.

   The logs indicate that the attacker (IP 154.53.63.93) is actively attempting to exploit **CVE-2023-20198** on a Cisco device (172.16.17.101) by bypassing authentication on its web interface. They are using various `curl` commands to probe the device and attempt to forge or manipulate session tokens to gain unauthorized access. Although the initial requests resulted in errors, the final request returned a session-like token, suggesting that the attack may be moving toward successful exploitation.

   This incident needs immediate containment and remediation, including blocking the source IP and applying the security patch to address **CVE-2023-20198**.

- **The Attack Were Successful.**

Attack Type: Authentication Bypass (related to CVE-2023-20198)

Attack Vector: Other

Reasoning:

1. **Log1 & Log2:**
    - The firewall allowed communication from the attacker (IP 154.53.63.93) to the internal device (172.16.17.101) over port 443 (HTTPS).
    - **Log2** from Snort shows an **authentication bypass attempt** for **Cisco IOS XE Web UI**. This indicates the attacker is trying to exploit **CVE-2023-20198**, which is an authentication bypass vulnerability in Cisco's Web UI, allowing attackers to gain unauthorized access to administrative functions without valid credentials.

    This is the key clue that the attack involves an **authentication bypass** rather than a typical injection attack.

2. **Log3:**
    - The attacker used a `curl` request with the encoded character `%25`. This could be a probing attempt, likely trying to test if the system has vulnerabilities in URL encoding or input handling. However, the request returned a `404 Not Found`, meaning it wasn't successful in accessing any resources.

    This log indicates the attacker was exploring the system but didn't use any of the known injection techniques listed (like SQL injection, XSS, etc.).

3. **Log4:**
    - The `curl -X POST` request to `webui/logoutconfirm.html` with a parameter (`logon_hash=1`) suggests the attacker is attempting to manipulate the Web UI session or authentication mechanism, likely exploiting **CVE-2023-20198**. The response (an alphanumeric string) suggests that the server generated or returned a session token, which the attacker may use to bypass authentication.

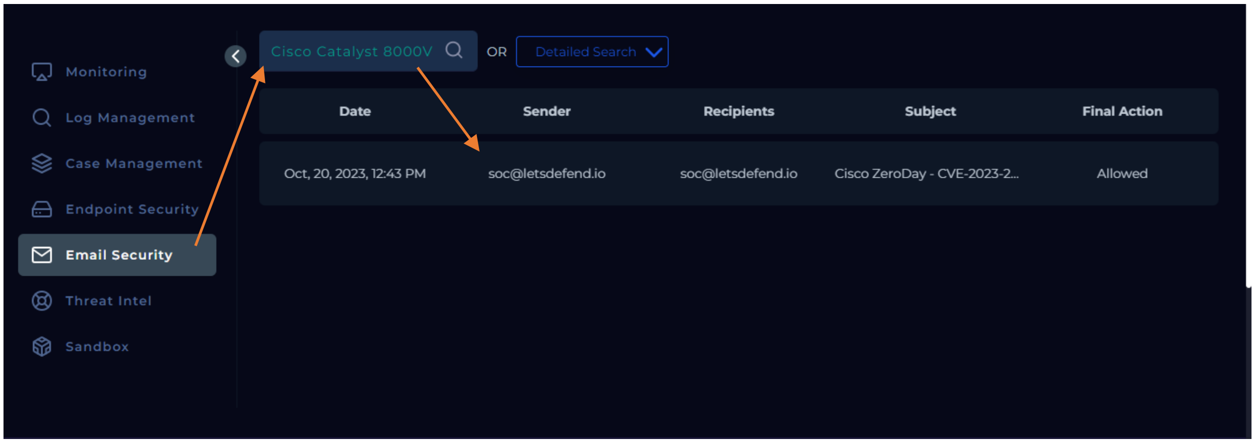
    Again, this indicates the attack vector is related to **authentication bypass** rather than any form of injection.

Why ?

1. **Not Command Injection:**
   The attacker is not injecting commands into a vulnerable application. They are trying to bypass authentication using web requests, not by inserting commands directly into an execution context.
2. **Not IDOR (Insecure Direct Object Reference):**
   The attacker isn’t trying to directly access unauthorized resources by modifying a reference. They are attempting to manipulate authentication using crafted HTTP requests.
3. **Not LFI & RFI (Local/Remote File Inclusion):**
   There are no signs of attempts to include or access local or remote files through URL manipulation.
4. **Not SQL Injection:**
   There is no evidence of SQL queries or attempts to manipulate a database in the logs. The attacker is focused on bypassing the web UI authentication.
5. **Not XML Injection:**
   XML-based data manipulation isn't involved here. No XML is seen in the logs.
6. **Not XSS (Cross-Site Scripting):**
   The attacker isn't trying to inject scripts into a web page. They are focused on backend authentication bypass via HTTP requests.

The attack is **an authentication bypass attempt** exploiting **CVE-2023-20198**, and the attack vector falls under "Other" since it doesn't fit into the traditional injection types like SQL, XML, or XSS.

Email Security:



Date	Sender	Recipients	Subject	Final Action
Oct, 20, 2023, 12:43 PM	soc@letsdefend.io	soc@letsdefend.io	Cisco ZeroDay - CVE-2023-2...	Allowed

- **Despite entering the source host name in the email security section, no emails have been sent, indicating that the attack was not executed.**
- **The Email appears it’s from L1 team.**

- ## The content of the Email.

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/

Please treat this matter with a sense of urgency, and we'll be relying on the expertise of Layer 2 to provide us with a clearer understanding of the situation.

We will remain vigilant and maintain continuous communication throughout the investigation.

Thank you for your immediate attention to this matter.

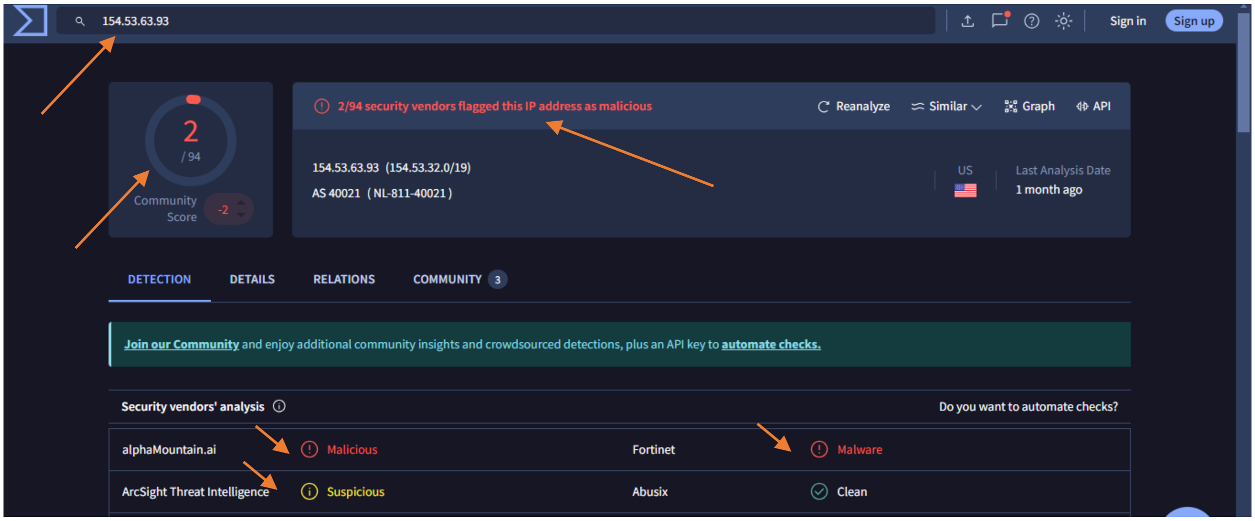
Sincerely,

Layer 1 Analyst

Detection:

Threat Intelligence Results

We will conduct a comprehensive scan of the source IP address using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



2/94 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
1 month ago

Join our 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	Fortinet	ⓘ Malware
ArcSight Threat Intelligence	ⓘ Suspicious	Abusix	✓ Clean

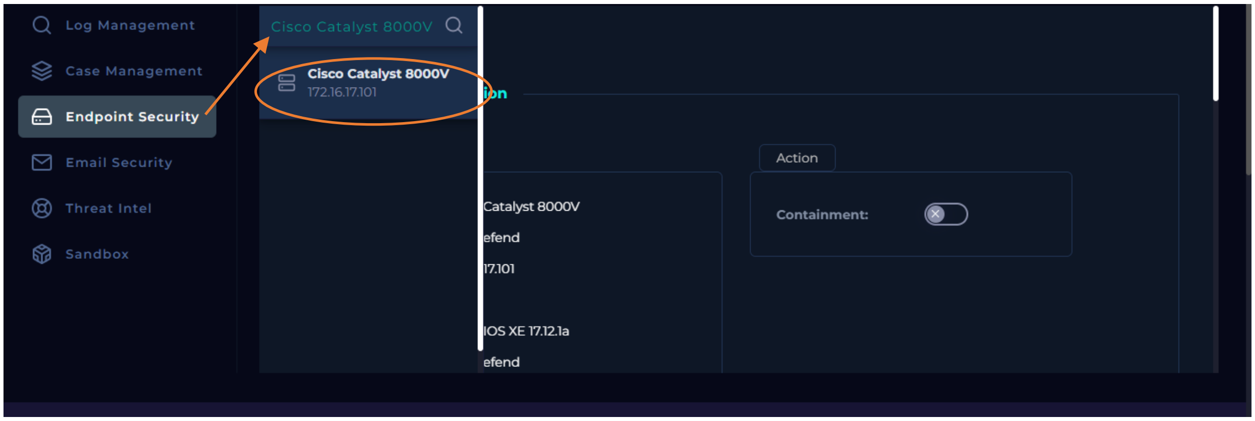
VirusTotal Results for Attacker IP: 154.53.63.93

Out of 94 security vendors, **2** flagged this IP address as **malicious**:

- **alphaMountain.ai:** Marked the IP as **Malicious**.
- **Fortinet:** Identified the IP as associated with **Malware**.
- **ArcSight Threat Intelligence:** Classified the IP as **Suspicious**.

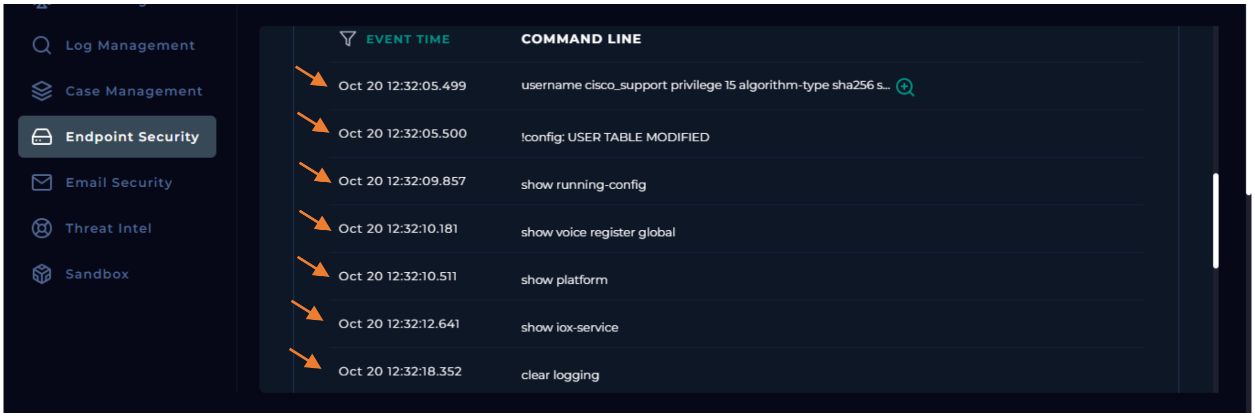
- **Reference result.**
- # The Traffic is Malicious

Endpoint Security:



Catalyst 8000V
efend
17.101
IOS XE 17.12.1a
efend

- We conducted a thorough review of the Terminal History, systematically analyzing each recorded entry step by step. Check the attached photo.



EVENT TIME	COMMAND LINE
Oct 20 12:32:05.499	username cisco_support privilege 15 algorithm-type sha256 s...
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

1. **Oct 20 12:32:05.499**

   ```
   username cisco_support privilege 15 algorithm-type sha256 secret *
   ```

   Explanation:
   The attacker is creating a new user (`cisco_support`) with **privilege level 15**, which is the highest privilege level on Cisco devices, granting full administrative access. The password is encrypted using the `sha256` algorithm.

   Implication:
   This shows that the attacker has already gained privileged access to the system (likely through the earlier authentication bypass) and is now creating a high-privilege user account. This is a critical step toward gaining persistent control over the device.

2. **Oct 20 12:32:05.500**

   ```
   !config: USER TABLE MODIFIED
   ```

   Explanation:
   The system is confirming that the user table has been modified, which validates the creation of the new user (`cisco_support`). The attacker has successfully created a backdoor account with administrative privileges.

3. **Oct 20 12:32:09.857**

   ```
   show running-config
   ```

   Explanation:
   The attacker is viewing the current running configuration of the device. This allows them to see the device’s settings, including network configurations, interfaces, routing, security policies, and possibly encrypted passwords.

   Implication:
   Accessing the running configuration indicates that the attacker is reviewing the system's settings to understand its structure and identify potential weaknesses or opportunities for further exploitation.

4. **Oct 20 12:32:10.181**

   ```
   show voice register global
   ```

   Explanation:
   This command is used to check the global voice registration settings, typically related to voice-over-IP (VoIP) systems. It shows the attacker's interest in exploring other services running on the device, possibly to exploit or gather further intelligence.

5. **Oct 20 12:32:10.511**

   ```
   show platform
   ```

   Explanation:
   This command provides detailed information about the hardware platform, including software versions, hardware components, and system resources. The attacker is gathering more system-level details.

6. **Oct 20 12:32:12.641**

   ```
   show iox-service
   ```

   Explanation:
   This command shows the status of Cisco's IOx services, which allow hosting applications on the router or switch. The attacker is likely checking for any running services that could be leveraged for further exploitation or persistent access.

7. **Oct 20 12:32:18.352**

   ```
   clear logging
   ```

   Explanation:
   The attacker is attempting to clear the device's logs. This is a common tactic used by attackers to cover their tracks and erase evidence of their presence on the device. It indicates that the attacker is trying to hide their activities from detection.

8. **Oct 20 12:32:22.515**

   ```
   no username cisco_support
   ```

   Explanation:
   The attacker is removing the `cisco_support` user they created earlier. This could be done to avoid detection after temporarily gaining control or after completing their actions.

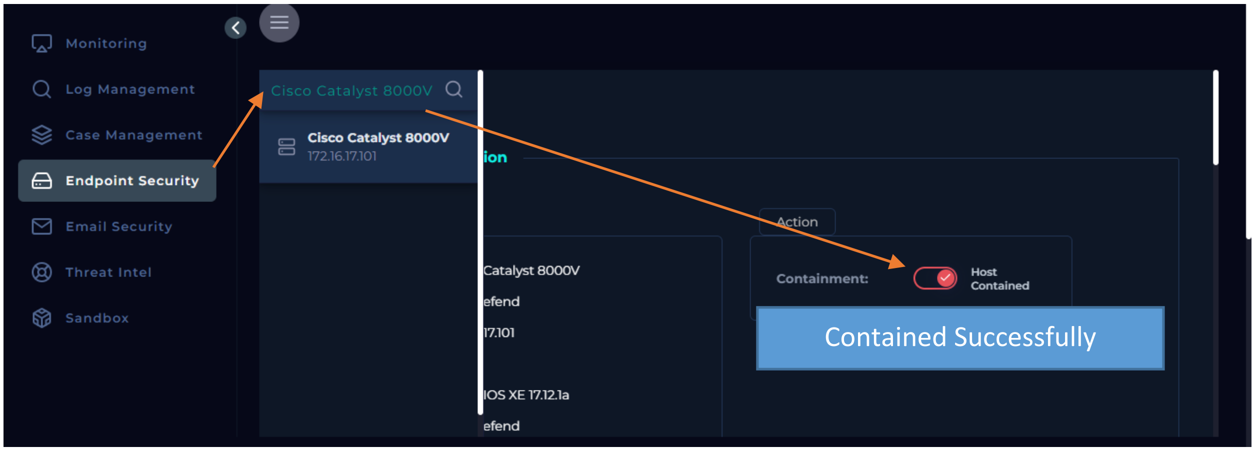
Analysis:

Based on the actions in these logs, the attacker **has gained full control** of the device. Here's why:

1. **Privilege Escalation:**
   The attacker successfully created a high-privilege user (`cisco_support`) with **privilege level 15**, the highest administrative access on a Cisco device. This alone demonstrates that they gained full control.
2. **Device Reconnaissance:**
   The commands such as `show running-config`, `show platform`, and `show iox-service` indicate that the attacker is exploring the system to gather information about its configuration and services, possibly to maintain persistence or launch further attacks.
3. **Covering Tracks:**
   The use of the `clear logging` command shows that the attacker is actively trying to erase evidence of their presence on the device, a sign that they have already completed their actions and want to remain undetected.
4. **User Removal:**
   Removing the `cisco_support` user could be another attempt to clean up and avoid leaving traces, after successfully gaining control and possibly extracting or modifying sensitive information.

   The attacker **gained full control of the device**. They created an administrative user, explored system settings, cleared logs, and removed the evidence of their created user. These are clear signs of a **successful attack** and the need for immediate remediation actions.

- **The device must be Contain. And we contained Successfully**.



Cisco Catalyst 8000V
172.16.17.101

Catalyst 8000V
efend
17.101
IOS XE 17.12.1a
efend

Containment: Host Contained

Conclusion:

On **October 20, 2023**, at 12:35 PM, an incident occurred involving the exploitation of **CVE-2023-20198**, targeting a **Cisco Catalyst 8000V** device within the network. The attacker, originating from an external IP address (**154.53.63.93**), leveraged an authentication bypass vulnerability in the **Cisco IOS XE Web UI** to gain unauthorized access. The firewall allowed initial communication over HTTPS, and subsequent Snort alerts indicated a targeted exploitation attempt aimed at bypassing the web interface's authentication mechanism.

Upon investigation of the logs, it became evident that the attacker utilized a series of HTTP requests, including encoded URL probes and POST requests, which ultimately resulted in a **session token** being generated. This token likely facilitated further unauthorized access, enabling the attacker to escalate privileges. The terminal history confirmed the creation of a high-privilege user account (**cisco_support**) with privilege level 15, granting full administrative control of the device.

The attacker executed multiple reconnaissance commands, such as reviewing the device's running configuration, exploring platform details, and checking services. This systematic exploration of the system was aimed at identifying weaknesses and ensuring persistence on the compromised device. Moreover, the attacker attempted to cover their tracks by clearing the system logs and eventually removing the newly created administrative account.

Given the observed activity, it is clear that the attacker gained **full control** over the device. The creation of a privileged account, execution of system commands, and subsequent log clearing all point to a **successful attack**. The attacker's actions were deliberate and strategic, demonstrating a clear intent to exploit the vulnerability for extended control and possibly further malicious activities.

Immediate remediation was essential. The source IP was flagged as malicious by multiple security vendors, and containment measures were implemented. The Cisco device was successfully contained, and further escalation has been made to ensure that all aspects of the incident are addressed comprehensively.

In conclusion, this incident highlights the critical nature of the CVE-2023-20198 vulnerability and the importance of timely patching and monitoring. The attacker's exploitation of this zero-day flaw allowed them to bypass authentication, escalate privileges, and manipulate the system undetected for a period of time. It is imperative that further analysis and remediation steps are conducted to ensure that no residual impacts remain and to safeguard the network from similar attacks in the future.