**Incident Summary:**

**Incident Name: Cisco IOS XE Vulnerability**

**Incident Date: October 11, 2023**

**Incident Analyst: Nagamani Chandrashekhar Gunjal**

**Incident Analyst UID: 121097675**

**Incident Analyst Section: 0101**

**Time Spent Analyzing Incident: 7 hours**

**Incident Summary:**

On October 11, 2023, a vulnerability in the Cisco IOS XE web UI feature was exploited, allowing an attacker with remote access to gain full control of the router using admin-level privileges. It was found that the router was compromised due to the CVE-2023-20198 vulnerability, which resulted from the web UI being exposed to the internet. The attacker first used CVE-2023-20198 to gain access and then escalated privileges using CVE-2023-20273. Logs were checked against Cisco’s IOCs, and vendor guidelines were followed to confirm the router's public exposure. Actions were taken to block malicious IPs, apply security patches, and secure public-facing interfaces. The organization also set up real-time monitoring to detect any further suspicious activity and reported findings to CISA to ensure a quick resolution.

**Incident Notes:**

**DETECT: How was the incident detected?**

The incident was detected by looking at the router.txt log file, where some unusual activities were noticed. The logs showed logins from a suspicious IP address and changes that matched the exploitation of vulnerabilities CVE-2023-20198 and CVE-2023-20273. It was also found that a public-facing router had its web UI exposed on port 443, which raised concerns about a possible compromise.

A close-up of a computer code

Description automatically generated

**ANALYSIS: What triage and analysis was performed?**

Logs analyzed the login events and found a WEBLOGIN\_SUCCESS entry showing access by the user **cisco\_support**, which is flagged as suspicious in Cisco advisories. Additionally, we noticed that the accounts **cisco\_tac\_admin** and **cisco\_support** were created with IP addresses outside the expected legitimate IP address ranges (5.149.249.74 and 154.53.56.231), which looked suspicious as the user created another user**.**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Using Splunk filter: *index="main" source="router.txt"* ***"%SEC\_LOGIN-5-WEBLOGIN\_SUCCESS****"* ***NOT netmri NOT steve***

Also, searched for login events while excluding known legitimate users (netmri, steve, and blairh). The filter confirmed that there were no traces of other users in the logs, indicating no unexpected or unauthorized login activity. There were always successful logins from legitimate users (**netmri, Steve, and blairh**) within the expected IP address ranges.

A screenshot of a computer

Description automatically generated

**Configuration Changes:** Logs showed a programmatic configuration update (%SYS-5-CONFIG\_P) by the process SEP\_webui\_wsma\_http, possibly initiated via the vulnerable web UI.

**index="main" source="router.txt" "%SYS-5-CONFIG\_P".** Logs were cross-referenced against known indicators of compromise (IoCs), including malicious IPs, filenames, and domains. The investigation also identified account creation and successful logins from a malicious IP address, but no other evidence of suspicious activity or IoCs was found in the logs.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

However, no relevant logs were found, indicating that there were no suspicious file installations or uploads detected on the router using the Splunk filter ***index="main" source="router.txt" "%WEBUI-6-INSTALL\_OPERATION\_INFO"***

**ANALYSIS: What Indicators of Compromise were discovered?**

* The unauthorized cisco\_support account was found on the router and flagged as malicious in Cisco advisories.
* A suspicious IP address, 154.53.56.231, was detected interacting with the router, matching known security threats.
* Updates made through SEP\_webui\_wsma\_http showed a possible exploitation of the web UI vulnerability, potentially giving an attacker full control of the system.

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

* The cisco\_support user account was removed from the router to prevent unauthorized access and secure the system.
* The Cisco IOS XE software was updated to the latest version to address vulnerabilities CVE-2023-20198 and CVE-2023-20273.
* Malicious IP addresses 154.53.56.231 and 5.149.249.74, flagged by multiple security sources, were blocked to prevent exploitation and protect the network.
* Public-facing web interfaces were secured by disabling unnecessary access and restricting it to trusted IP addresses only.
* Real-time monitoring and alerts were set up to detect unauthorized logins, configuration changes, and suspicious activities.

**RECOVERY: What recovery steps were taken?**

* The router’s configuration was restored to a secure state to eliminate any changes made during the compromise.
* The system was rebooted to remove any unauthorized sessions and start fresh.
* Continuous monitoring was implemented to catch any suspicious login attempts, configuration changes, or interactions with malicious IPs, keeping the system safe and secure.

**POST INCIDENT ACTIVITY: Lessons Learned / Follow up items**

* Turn off web interfaces on devices that don’t need internet access and limit access to trusted IP addresses only.
* Set up real-time alerts to catch any unauthorized logins, unexpected changes, or suspicious activities.
* Regularly check logs to spot any potential threats or unusual behavior.
* Apply important patches like CVE-2023-20198 and CVE-2023-20273 to keep the system secure.
* Renew software licenses on time to avoid issues like the SMART\_LIC-3-EVAL\_EXPIRED\_WARNING.

A screenshot of a computer

Description automatically generated

* Create incident response plans for Cisco-related security issues.
* Provide regular training for the team to quickly identify and respond to security incidents, and ensure every employee has access to playbooks with detailed information.