SECURITY ADVISORY

CISCO IOS XE CRITICAL SEVERITY ZERO DAY VULNERABILITY UNDER ACTIVE EXPLOITATION (CVE-2023-20198)

Lodestone Security

OCTOBER 17TH 2023

Table of Contents

Executive Summary

On Monday, October 16th, 2023, Cisco's Product Security Incident Response Team (PSIRT) released an advisory concerning a critical severity vulnerability (CVSS Base score of 10.0). This vulnerability, known to be actively exploited in the wild, is associated with the Web User Interface (Web UI) feature of Cisco IOS XE software. This vulnerability is of particular concern when the software is exposed to the internet or untrusted networks. The vulnerability has been assigned CVE-2023-20198.

The vulnerability enables a remote, unauthenticated attacker to establish an account on the affected system with full administrator privileges, known in Cisco IOS as "level 15 access."

As of this writing, Cisco has confirmed active exploitations of this vulnerability. Threat actors are leveraging it to deploy "implants" on affected systems, thereby granting them the capability to remotely execute arbitrary commands on these systems and use them to move laterally within networks or stage further attacks.

Organizations with deployed Cisco IOS XE Products should ensure the Web UIs of these products are segmented internally and accessible solely to specified management networks. Any organization with Cisco IOS XE Products, where the Web UIs are directly accessible from the internet, should urgently restrict access to HTTP(S) on these systems. Organizations with Cisco IOS XE deployed should follow the mitigation steps outlined in the "Mitigations/Workarounds" section of the advisory.

Affected Systems / Products

This vulnerability affects Cisco IOS XE software if the web UI feature is enabled. Organizations where this Web UI is directly exposed to the internet should react immediately and work to evaluate the integrity of their devices.

To validate if the Web UI is enabled on Cisco IOS XE products, administrators with Command Line (CLI) access can execute the following commands:

```
show running-config | include ip http server|secure|active
```

If the system has the HTTP Server featured enabled, the preceding command will output **either or both lines**:

```
ip http server

ip http secure-server
```

The presence of **either** "ip http server" or "ip http secure-sever" indicate that your system is likely vulnerable to this issue and you should take immediate action to mitigate the vulnerability by following the instructions in the "Mitigations / Workarounds" section of this advisory.

Mitigations / Workarounds

Organizations with Cisco products that run IOS XE should **temporarily** mitigate this issue by disabling the Web UI on affected products.

However, it's important to note that disabling the Web UI may disrupt services that require HTTP / HTTPS communication, such as Cisco Embedded Wireless Controller (eWLC).

To disable the HTTP Server feature issue both of the following commands in global configuration mode (configure-terminal):

```
no ip http server
no ip http secure-server
```

Note: It is recommended that administrators save the back up the "running" and "startup" configurations of production networking infrastructure PRIOR to running the commands above to disable the vulnerable Web UI.

Additionally, after running the commands above, administrators should save the configuration to ensure restarting any affected systems does not inadvertently re-enable the vulnerable Web UI:

```
copy running-configuration startup-configuration
```

Patches

At the time of writing, there are currently **NO** patches available for this vulnerability.

However, Threat actors have **also** been observed leveraging the already patched CVE-2021-1435, to install the implant **after successful exploitation of CVE-2023-20198**.

Indicators of Compromise (IOCs)

Organizations that believe they may have Cisco IOS XE systems that were directly exposed to the internet should leverage the following Indicators of Compromise (IOCs) to identify potential signs of successful exploitation.

Successful exploitation of CVE-2023-20198 allows threat actors to create privileged accounts on impacted systems. At the time of this writing, Cisco has communicated that they have observed threat actors creating accounts with the following usernames on successfully exploited systems:

```
cisco_tac_admin
cisco_support
```

Note: While threat actors have the capability to create user accounts with ANY username, the ones listed above are those currently observed in active exploits of this vulnerability. Organizations should review their Cisco IOS XE logs for the creation of ANY new users that are not recognized by their system administrators.

Organizations should conduct the following further checks in system logs to determine if a device may be compromised:

Check for the presence of any of the following log messages in which "user" could be "cisco_tac_admin", "cisco_support", or **any unknown** local user configured:

```
%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 $DATE
```

Note: The log messages described above will be logged every time a user successfully authenticates to the Web UI. The goal is to look for successful logins by user accounts that are unknown to system administrators and likely created recently.

Check for the presence of the following message, which may be indicative of an attacker deploying the implant after successful exploitation, particularly if the "filename" is unknown to the system administrator.

```
%WEBUI-6-INSTALL_OPERATION_INFO: User: username, Install Operation: ADD filename
```

How Lodestone is Responding

Lodestone is exploring methods for KARMA Attack Surface Management to effectively detect the presence of Cisco IOS XE Web UIs on internet-facing infrastructure, with the aim of notifying potentially affected organizations currently being scanned by KARMA.

Sources

https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
https://nvd.nist.gov/vuln/detail/CVE-2023-20198