Security Advisory 2023-078

Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

October 17, 2023 — v1.1

TLP:CLEAR

History:

- *17/10/2023 — v1.0 – Initial publication*
- *23/10/2023 — v.1.1 – Added information about a new vulnerability and available updates*

Summary

On October 16 2023, Cisco published an advisory regarding a critical vulnerability, **CVE-2023-20198**, affecting the Web UI of Cisco IOS XE Software. This vulnerability could allow an unauthenticated remote attacker to create a privileged level 15 account, granting them control over the affected system.

[UPDATE] On October 20 2023, Cisco identified an additional vulnerability **CVE-2023-20273**, which, when exploited, affects another component of the web UI feature. This vulnerability allows the new local user to elevate its privilege to root and write an implant to the file system. [1]

- **CVE-2023-20198** has been assigned a CVSS Score of 10.0.
- **CVE-2023-20273** has been assigned a CVSS Score of 7.2.

Cisco has released software updates that address the vulnerabilities described in this advisory [1]. It is also advised to implement the recommendations.

Technical Details

The vulnerability `CVE-2023-20198` allows a remote, unauthenticated attacker to exploit the web UI feature of Cisco IOS XE Software, enabling them to create an account with privilege level 15 access.

The vulnerability `CVE-2023-20273` allows the new local user to elevate its privilege to root and write an implant to the file system.

Affected Products

This vulnerability affects Cisco IOS XE Software if the web UI feature is enabled. The web UI feature is enabled through the `ip http server` or `ip http secure-server` commands [1].

To check if the web UI feature is enabled, look for `ip http server` and `ip http secure-server` in the system configuration.

Detection

To determine whether a system may have been compromised, perform the following checks [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 Wed Oct 11 2023
```

Note: The `%SYS-5-CONFIG_P` message will be present for each instance that a user has accessed the web UI. The indicator to look for is new or unknown usernames present in the message.

Check the system logs for the following message where `filename` is an unknown filename that does not correlate with an expected file installation action:

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

Cisco Talos has provided the following command to check for the presence of the implant where systemip is the IP address of the system to check. This command should be issued from a workstation with access to the targeted system (if the system is configured for HTTP access only, use the HTTP scheme in the command below):

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

If the request returns a hexadecimal string, the implant is present.

Workarounds

There are no workarounds that address these vulnerabilities.

Recommendations

CERT-EU recommends disabling the HTTP Server feature on all internet-facing systems and scanning affected devices for the presence of indicators of compromise (IoCs). [1]

[UPDATE] CERT-EU strongly recommends updating affected devices. The first fixed software releases have been posted on the Cisco Software Download Center, and additional releases will be made available. [2]

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

[2] https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-dublin-17121/221128-software-fix-availability-for-cisco-ios.html