aDvens

Security for the greater good

Newscast

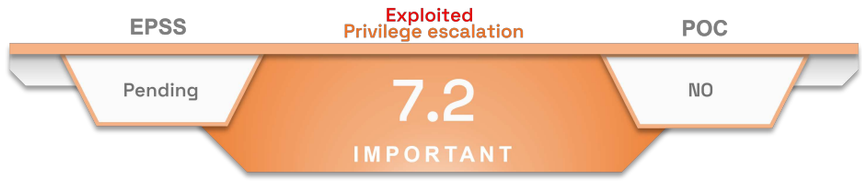
Critical vulnerability in CISCO IOS XE

2023-10-23 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-20273 (Exploited)



On 20 October 2023, *Cisco* updated a security advisory to indicate the discovery of a new 0-day: CVE-2023-20273. This vulnerability can be exploited following a compromise via CVE-2023-20198.

It allows an authenticated attacker to exploit a flaw in the web user interface to inject commands with *root* privileges and execute arbitrary code.

This vulnerability is being exploited. Talos Intelligence has observed the exploitation of this vulnerability, following a primary infection via CVE-2023-20198, in order to install LUA implants.

Risk

- Privilege escalation
- Remote code execution

Severity (Base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	High	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Product

The following versions of Cisco IOS XE when the user interface is enabled:

- versions 16.12 (only Catalyst 3650 and 3850)
- versions 17.3
- versions 17.6
- versions 17.9

Recommendations

aDvens' CERT recommends testing proposed workaround measures in a test environment before deploying them in production. This step is crucial to prevent any unintended side effects.

Fix

- Update Cisco IOS XE versions 17.9 to version 17.9.4.
- Further updates will be published shortly. You can keep up to date by monitoring the dedicated Cisco advisory.
- Additional information is available on the editor's website.

Decision tree

Below, a decision tree proposed by the editor.

Are you running IOS XE?

- No. The system is not vulnerable. No further action is necessary.
- Yes.

If yes, is ip http server or ip http secure-server configured?

- No. The vulnerability is not exploitable. No further action is necessary.
- Yes.

If yes, do you run services that require HTTP/HTTPS communication (for example, eWLC)?

- No. Disable the HTTP Server feature.
- Yes.

If yes, restrict if possible the access to those services to trusted networks.

When implementing access controls for these services, be sure to review the controls because there is the potential for an interruption in production services. If you are unsure of these steps, work with your support organization to determine appropriate control measures.

After implementing any changes, run the copy running-configuration startup-configuration command to save the running-configuration. This will ensure that the changes are not reverted in the event of a system reload.

CISA

CISA recommends reading the following documentation

- BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities

Proof of concept

To date, no proof of concept is available in open source.

Indicators of Compromise

Check system logs

To determine whether a system may have been compromised, perform the following checks:

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
```

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
```

Check the presence of an implant

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 system in question:

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

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

If the system is configured for HTTP access only, use the HTTP scheme in the command example.

The following Snort rule IDs are also available to detect exploitation

- 3:50118:2 - can alert for initial implant injection
- 3:62527:1 - can alert for implant interaction
- 3:62528:1 - can alert for implant interaction
- 3:62529:1 - can alert for implant interaction

TLP	TYPE	VALUE
TLP:CLEAR	IP	5.149.249.74
TLP:CLEAR	IP	154.53.56.231
TLP:CLEAR	IP	154.53.63.93
TLP:CLEAR	username	cisco_tac_admin
TLP:CLEAR	username	cisco_support
TLP:CLEAR	username	cisco_sys_manager

Sources

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
- 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
- https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/