Security for the greater good

Newscast

Critical vulnerability in CISCO IOS XE

2023-10-31 I **TLP:CLEAR** I CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

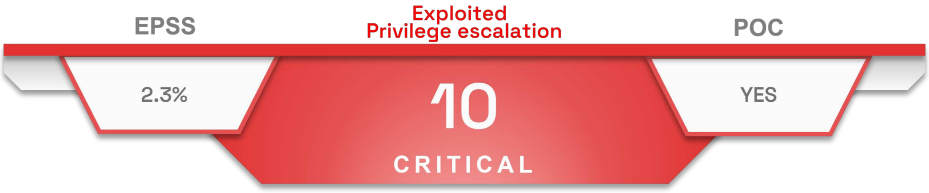
Table of content

CVE-2023-20198 (EXPLOITED) **2**

- **Type of vulnerability** **2**
- **Risk** **2**
- **Severity (base score CVSS 3.1)** **2**
- **Impacted Product** **2**
- **Recommendations** **2**
  - Fix 2
  - Decision tree 3
  - CISA 3
  - Indicator of Compromise 3
  - Check system logs 3
  - Check the presence of an implant 4
- **Proof of concept** **4**

SOURCES **5**

CVE-2023-20198 (Exploited)



On 16 October 2023, *Cisco* published a security advisory concerning the discovery of CVE-2023-20198: a critical and actively exploited vulnerability that affects the web user interface of *IOS XE*.

Update from 31 october 2023: This vulnerability stems from a lack of control of user supplied data allowing an attacker to bypass Nginx matches.

Update from 31 october 2023: By sending a specially crafted request, a remote and unauthenticated attacker can gain access to the *wsma* service, without going through *WSMASendCommand* (that verifies the user is authenticated), allowing him to execute arbitrary commands, modify the system configuration and create a new user account with level 15 privileges on the vulnerable system.

> This vulnerability is exploited.
> Update from 31 october 2023: On 25 october, Censys estimates that **28,000 Cisco devices** exposed on the internet show signs of comprimise.

Type of vulnerability

CWE-269 : Improper Privilege Management

Risk

- Privilege escalation

Severity (base score CVSS 3.1)

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

Impacted Product

- Cisco IOS XE Software : if the *web UI* feature is enabled.

Recommendations

Fix

- Update from 31 october 2023: Update Cisco IOS XE to version 16.12.10a, 17.3.8a, 17.6.5a, 17.6.6a, 17.9.4a or later. Update 17.12.2 is planned to be released on 15 november 2023. More information concerning these updates is available in Cisco's dedicated advisory.
- Additional information is available on the editor's website.

Decision tree

Below, a decision tree presented 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

Indicator 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

Proof of concept

> Update from 31 october 2023: A proof of concept is available in open source since 30 october 2023.

Sources

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
- https://nvd.nist.gov/vuln/detail/CVE-2023-20198
- https://www.cybersecurity-help.cz/vdb/SB2023101701
- https://exchange.xforce.ibmcloud.com/vulnerabilities/268681
- 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://www.cisa.gov/guidance-addressing-cisco-ios-xe-web-ui-vulnerabilities
- https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/