Cisco Security Advisory

Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature

Critical

Advisory ID:	cisco-sa-iosxe-webui-privesc-j22SaA4z	CVE-2023-20198
First Published:	2023 October 16 15:00 GMT	CVE-2023-20273
Last Updated:	2023 November 1 15:44 GMT	CWE-420
Version 2.6:	Final	CWE-78
Workarounds:	No workarounds available	
Cisco Bug IDs:	CSCwh87343	
CVSS Score:	Base 10.0	

Download CSAF

Email

Summary

Cisco is providing an update for the ongoing investigation into observed exploitation of the web UI feature in Cisco IOS XE Software. We are updating the list of fixed releases and adding the Software Checker.

Fix information can be found in the Fixed Software section of this advisory.

Our investigation has determined that the actors exploited two previously unknown issues.

The attacker first exploited CVE-2023-20198 to gain initial access and issued a privilege 15 command to create a local user and password combination. This allowed the user to log in with normal user access.

The attacker then exploited another component of the web UI feature, leveraging the new local user to elevate privilege to *root* and write the implant to the file system. Cisco has assigned CVE-2023-20273 to this issue.

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

Both of these CVEs are being tracked by CSCwh87343.

For steps to close the attack vector for these vulnerabilities, see the Recommendations section of this advisory.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Affected Products

Vulnerable Products

These vulnerabilities affect 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.

Determine the HTTP Server Configuration

To determine whether the HTTP Server feature is enabled for a system, log in to the system and use the **show running-config | include ip http server|secure|active** command in the CLI to check for the presence of the **ip http server** command or the **ip http secure-server** command in the global

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Related to This Advisory

Your Rating:

Average Rating:

5 star 4
4 star 0
3 star 0
2 star 0
1 star 0

Leave additional feedback

Feedback

configuration. If either command is present, the HTTP Server feature is enabled for the system.

The following example shows the output of the **show running-config | include ip http server|secure|active** command for a system that has the HTTP Server feature enabled:

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

Note: The presence of either command or both commands in the system configuration indicates that the web UI feature is enabled.

If the **ip http server** command is present and the configuration also contains **ip http active-session-modules none**, these vulnerabilities are not exploitable over HTTP.

If the **ip http secure-server** command is present and the configuration also contains **ip http secure-active-session-modules none**, these vulnerabilities are not exploitable over HTTPS.

Products Confirmed Not Vulnerable

Cisco has confirmed that these vulnerabilities do not affect the following Cisco products:

- Adaptive Security Appliance (ASA) Software
- Firepower Threat Defense (FTD) Software
- Identity Services Engine (ISE)
- IOS Software
- IOS XE Software prior to Release 16
- NX-OS Software

Details

The web UI is an embedded GUI-based system-management tool that provides the ability to provision the system, to simplify system deployment and manageability, and to enhance the user experience. It comes with the default image, so there is no need to enable anything or install any license on the system. The web UI can be used to build configurations as well as to monitor and troubleshoot the system without CLI expertise.

Indicators of Compromise

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
```

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 system in question:

```
curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e9bb" -X
POST "https://systemip/webui/logoutconfirm.html?logon_hash=1"
```

If the request returns a hexadecimal string such as **0123456789abcdef01**, the implant is present.

Note: The above command should be entered as a single command line.

Note: 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 - alerts for initial implant injection (CVE-2023-20273)
- 3:62527 - alerts for implant interaction
- 3:62528 - alerts for implant interaction
- 3:62529 - alerts for implant interaction
- 3:62541 - alerts on attempted exploitation for initial access (CVE-2023-20198)
- 3:62542 - alerts on attempted exploitation for initial access (CVE-2023-20198)

Workarounds

There are no workarounds that address these vulnerabilities.

Disabling the HTTP Server feature eliminates the attack vector for these vulnerabilities and may be a suitable mitigation until affected devices can be upgraded. Administrators can disable the HTTP Server feature by using the **no ip http server** or **no ip http secure-server** command in global configuration mode. If both *http server* and *http-secure server* are in use, then both commands are required to disable the HTTP Server feature.

Limiting access to the HTTP Server to trusted networks will limit exposure to these vulnerabilities. The following example shows how to allow remote access to the HTTP Server from the trusted 192.168.0.0/24 network:

```
!
ip http access-class 75
ip http secure-server
!
access-list 75 permit 192.168.0.0 0.0.0.255
access-list 75 deny   any
!
```

Note: To apply the access list in newer versions of Cisco IOS XE Software, use the **ip http access-class ipv4 75** command for the previous example. See Filter Traffic Destined to Cisco IOS XE Devices WebUI Using an Access List for additional information.

While this mitigation has been deployed and was proven successful in a test environment, customers should determine the applicability and effectiveness in their own environment and under their own use conditions. Customers should be aware that any workaround or mitigation that is implemented may negatively impact the functionality or performance of their network based on intrinsic customer deployment scenarios and limitations. Customers should not deploy any workarounds or mitigations before first evaluating the applicability to their own environment and any impact to such environment.

Fixed Software

Cisco has released free software updates that address the vulnerabilities described in this advisory. Customers with service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license:
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool.

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco TAC:
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

Fixed Releases

Customers are advised to upgrade to an appropriate fixed software release as indicated in the following table:

Cisco IOS XE Software Release Train	First Fixed Release	Available
17.9	17.9.4a	Yes
17.6	17.6.6a	Yes
17.3	17.3.8a	Yes
16.12 (Catalyst 3650 and 3850 only)	16.12.10a	Yes

The SMUs in the following table address Cisco Bug ID CSCwh87343:

Cisco IOS XE Software Release Train	Base Release	SMU Available
17.9	17.9.4	Yes
17.6	17.6.5	Yes

For detailed platform release information, see Software Fix Availability for Cisco IOS XE Software Web UI Privilege Escalation Vulnerability - CVE-2023-20198.

Cisco IOS and IOS XE Software

To help customers determine their exposure to vulnerabilities in Cisco IOS and IOS XE Software, Cisco provides the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific software release and the earliest release that fixes the vulnerabilities that are described in each advisory ("First Fixed"). If applicable, the tool also returns the earliest release that fixes all the vulnerabilities that are described in all the advisories that the Software Checker identifies ("Combined First Fixed").

To use the tool, go to the Cisco Software Checker page and follow the instructions. Alternatively, use the following form to determine whether a release is affected by any Cisco Security Advisory. To use the form, follow these steps:

1. Choose which advisories the tool will search–only this advisory, only advisories with a Critical or High Security Impact Rating (SIR), or all advisories.
2. Enter a release number–for example, 15.9(3)M2 or 17.3.3.
3. Click **Check**.

Only this advisory

Enter release number Check

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

Recommendations

Cisco strongly recommends that customers disable the HTTP Server feature on all internet-facing systems or restrict its access to trusted source addresses. To disable the HTTP Server feature, use the **no ip http server** or **no ip http secure-server** command in global configuration mode. If both the HTTP server and HTTPS server are in use, both commands are required to disable the HTTP Server feature.

The following decision tree can be used to help determine how to triage an environment and deploy protections:

- Are you running IOS XE?
  - **No**. The system is not vulnerable. No further action is necessary.
  - **Yes**. Is **ip http server** or **ip http secure-server** configured?
    - **No**. The vulnerabilities are not exploitable. No further action is necessary.
    - **Yes**. Do you run services that require HTTP/HTTPS communication (for example, eWLC)?
      - **No**. Disable the HTTP Server feature.
      - **Yes**. If possible, restrict access to those services to trusted networks.

We assess with high confidence, based on further understanding of the exploit, that access lists applied to the HTTP Server feature to restrict access from untrusted hosts and networks are an effective mitigation.

When implementing access controls for these services, as per the mitigations provided, 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, use 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.

For additional information on the impact of disabling the HTTP Server feature, see Cisco TAC Technical FAQs for Cisco IOS XE Software Web UI Privilege Escalation Vulnerability - CVE-2023-20198.

Exploitation and Public Announcements

Cisco is aware of active exploitation of these vulnerabilities.

Source

These vulnerabilities were found during the resolution of multiple Cisco TAC support cases.

URL

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

Revision History

Version	Description	Section	Status	Date
2.6	Updated the list of products confirmed not vulnerable.	Affected Products	Final	2023-NOV-01
2.5	Updated fixed release table and added software checker and updated summary to reflect these changes.	Summary and Fixed Software	Final	2023-OCT-31

Show Complete History...