

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Unpatched Zero-Day Vulnerability Actively Exploited in Cisco IOS XE

Date of Publication

October 17, 2023

Last Update Date

October 23, 2023

Admiralty Code

A1

TA Number

TA2023420







Summary

First Seen: October 16, 2023

Affected Products: Cisco IOS XE Software

Impact: The critical, unpatched security vulnerability identified as CVE-2023-20198 affects Cisco IOS XE software. Cisco IOS XE is a network operating system used in Cisco network devices. The identified flaw is an authentication bypass zero-day vulnerability within the IOS XE software and is actively exploited in the wild. This vulnerability enables unauthenticated attackers to obtain full administrator privileges and take remote control of affected Cisco routers and switches.

CVEs

| CVE | NAME | AFFECTED PRODUCT | ZERO -DAY | CISA KEV | PATCH |
|----------------|--|-----------------------|---|---|---|
| CVE-2023-20198 | Cisco IOS XE Web UI Privilege Escalation Vulnerability | Cisco IOS XE Software |  |  |  |
| CVE-2023-20273 | Cisco IOS XE Web UI Arbitrary Code Execution Vulnerability | Cisco IOS XE Software |  |  |  |

Vulnerability Details

#1

A critical zero-day vulnerability, identified as CVE-2023-20198, has been discovered in Cisco IOS XE software, a network operating system used in Cisco routers and switches. The flaw allows unauthenticated attackers to gain full administrator privileges, enabling them to assume complete control of vulnerable routers and switches from a remote location. The critical flaw is limited to devices running with the Web UI feature enabled.

#2

The successful exploitation of CVE-2023-20198 enables an attacker to create an account on the affected device with privilege level 15 access. This is a significant concern because privilege level 15 essentially grants full control of the compromised device.

#3

The attacks exploiting CVE-2023-20198 were first detected in September 2023. The attacker created a local user account named "cisco_tac_admin" from a suspicious IP address and in a recent attack attackers were found to be creating different account named "cisco_support" from a different IP address. The attackers also deployed a malicious Lua implant, which allowed them to execute arbitrary commands with elevated (root) privileges at the system or IOS levels by exploiting a second vulnerability, CVE-2023-20273. It's worth noting that the implant becomes active once the web service is restarted, however it lacks persistence and shall be removed on device restart.

#4

Initially, over 50,000 devices were found infected with the implants. However, within a few days of discovery, the number dramatically dropped from around 60,000 to less than 1000 devices. This decline suggests that the threat actors responsible for the attacks likely took measures to conceal their presence and avoid detection. This could involve deploying updates or making changes to their tactics.

#5

Cisco has released fixes for SDWAN and IOT technologies for version 17.9.4a and is actively working on patches for other versions and affected product. Additionally, Cisco has also provided mitigation steps including disabling of the HTTP server feature and has provided snort rules for detecting any exploit attempt.

Vulnerabilities

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|----------------|----------------------------|--|---------|
| CVE-2023-20198 | Cisco IOS XE- All versions | cpe:2.3:o:cisco_systems:cisco_ios_xe:*:*:*:*:* | CWE-269 |
| CVE-2023-20273 | Cisco IOS XE- All versions | cpe:2.3:o:cisco_systems:cisco_ios_xe:*:*:*:*:* | CWE-78 |

Recommendations



Disable the HTTP server feature: Admins are strongly advised to take proactive measures to secure their systems in light of this critical vulnerability being exploited. Disabling the HTTP server feature on internet-facing systems is a key step to eliminate the attack vector and effectively block incoming attacks.



Limit Service Exposure: Consider limiting web UI service exposure to specific trusted networks to reduce the attack surface and minimize service exposure to potential threats.



Monitor User Accounts: Utilize automated systems for System Event Monitoring, ensuring constant surveillance of account creation activities in real time. The monitoring platform should be capable of instantly notifying administrators or security teams upon detecting any suspicious activities.

Potential MITRE ATT&CK TTPs

| | | | |
|--|--|--|---|
| <u>TA0042</u> Resource Development | <u>TA0001</u> Initial Access | <u>TA0002</u> Execution | <u>TA0003</u> Persistence |
| <u>TA0004</u> Privilege Escalation | <u>TA0005</u> Defense Evasion | <u>T1588</u> Obtain Capabilities | <u>T1588.006</u> Vulnerabilities |
| <u>T1136.001</u> Local Account | <u>T1068</u> Exploitation for Privilege Escalation | <u>T1059</u> Command and Scripting Interpreter | <u>T1059.008</u> Network Device CLI |
| <u>T1190</u> Exploit Public-Facing Application | <u>T1136</u> Create Account | | |

✂ Indicators of Compromise (IOCs)

| TYPE | VALUE |
|----------|---|
| IPv4 | 5.149.249[.]74, 154.53.56[.]231, 154.53.63[.]93 |
| Username | cisco_tac_admin, cisco_support, cisco_sys_manager |

✂ Mitigations

Cisco has **recommended** to disable the HTTP Server feature on all internet-facing systems as a proactive step to enhance security in light of the CVE-2023-20198 vulnerability. Use following command in global configuration mode to disable the HTTP Server feature, 'no ip http server' and 'no ip http secure-server'.

✂ Patch Details

Cisco has released patches for SD-WAN and IoT technologies for version 17.9.4a and is actively working on patches for other services.

Link:

<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>

✂ References

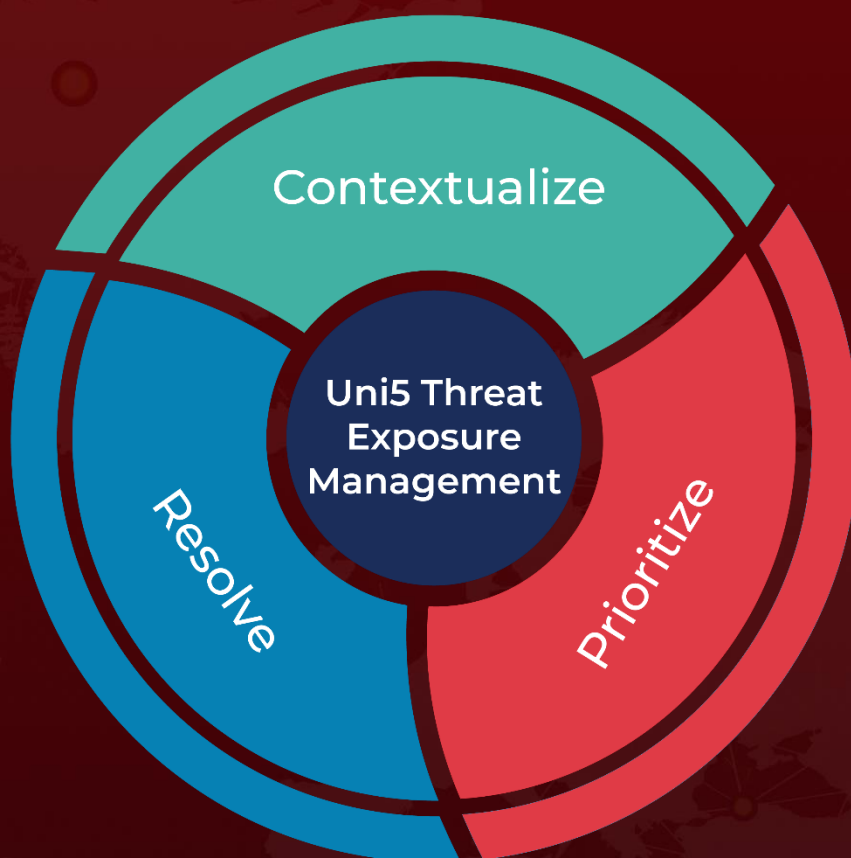
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z>

<https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

October 17, 2023 • 6:25 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com