



# Cisco IOS XE Web UI Privilege Escalation Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-20198
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-16 16:15:00 UTC
<b>Updated</b>	2024-01-25 17:15:00 UTC
<b>Description</b>	Cisco is providing an update for the ongoing investigation into observed exploitation of the web UI feature in Cisco IOS XE : 

## Risk And Classification

**EPSS:** 0.940130000 probability, percentile 0.998940000 (date 2026-04-03)

**CISA KEV:** Listed on 2023-10-16; due 2023-10-20; ransomware use Unknown

**Problem Types:** NVD-CWE-noinfo

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	IOS XE Web UI
<b>Name</b>	Cisco IOS XE Web UI Privilege Escalation Vulnerability
<b>Required Action</b>	Verify that instances of Cisco IOS XE Web UI are in compliance with BOD 23-02 and apply mitigations per vendor instructions. For affected products (Cisco IOS XE Web UI exposed to the internet or to untrusted networks), follow vendor instructions to determine if a system may have been compromised and immediately report positive findings to CISA.
<b>Notes</b>	<a href="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.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-dublin-17121/221128-software-fix-availability-for-cisco-ios.html</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-20198">https://nvd.nist.gov/vuln/detail/CVE-2023-20198</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios Xe	All	All	All	All

## References

Reference	Source	Link	
Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities   CISA	MISC	<a href="http://www.cisa.gov">www.cisa.gov</a>	1
Actively exploited Cisco 0-day with maximum 10 severity gives full network control   Ars Technica	MISC	<a href="http://arstechnica.com">arstechnica.com</a>	

Critical, Unpatched Cisco Zero-Day Bug Is Under Active Exploit	MISC	<a href="http://www.darkreading.com">www.darkreading.com</a>
<a href="https://packetstormsecurity.com/files/175674/Cisco-IOX-XE-Unauthenticated-Remote-Code-Executi...">packetstormsecurity.com/files/175674/Cisco-IOX-XE-Unauthenticated-Remote-Code-Executi...</a>		<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>
Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature	MISC	<a href="https://sec.cloudapps.cisco.com">sec.cloudapps.cisco.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="http://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[150739](#) Cisco IOS XE Web UI Privilege Escalation Vulnerability (CVE-2023-20198)

[317376](#) Cisco Internetwork Operating System (IOS) XE Software Web UI Privilege Escalation Vulnerability (cisco-sa-iosxe-webui-privesc-j22SaA4z)

[730965](#) Cisco Internetwork Operating System (IOS) XE Software Web UI Privilege Escalation Vulnerability (cisco-sa-iosxe-webui-privesc-j22SaA4z) (Unauthenticated Check)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)