Cisco IOS XE Web UI Privilege Escalation Vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-20198
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-16 16:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	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

Vendor	Cisco
Product	IOS XE Web UI
Name	Cisco IOS XE Web UI Privilege Escalation Vulnerability
Required Action	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.
Notes	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://nvd.nist.gov/vuln/detail/CVE-2023-20198

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	www.cisa.gov
Actively exploited Cisco 0-day with maximum 10 severity gives full network control | Ars Technica	MISC	arstechnica.com

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

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)