

Cisco IOS XE Web UI Attack

Multiple 0-Day vulnerabilities on Cisco IOS XE Web UI

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z>
 CVEs: CVE-2023-20198, CVE-2023-20273

Active exploitation of a previously unknown vulnerabilities in the Web User Interface (Web UI) of Cisco IOS XE software when exposed to the internet or untrusted networks. According to open source articles, thousands of vulnerable devices have been compromised.

Background Cisco IOS XE is the internetworking operating system used by the Next-Generation Cisco Systems such as routers and switches. The Web User Interface (WebUI) provides simplified deployment and manageability of the devices.

According to the vendor report, this vulnerability (CVE-2023-20198) allows a remote, unauthenticated attacker to create an account on an affected system. The attacker can then use that account to gain control of the affected system including installing a backdoor.

Next, the attacker can use the new unauthorized local user account to exploit a second previously unknown vulnerability (CVE-2023-20273) in another component of the WebUI feature. This allows the adversary to inject commands with elevated (root) privileges, giving them the ability to run arbitrary commands on the device.

Announced Oct 16, 2023: Cisco released an advisory for CVE-2023-20198
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z>

Oct 16, 2023: Cisco Talos released a detailed blog about the CVE-2023-20198 vulnerability and its active exploitation.
<https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/>

Oct 16, 2023: FortiGuard Labs released a Threat Signal for the vulnerability (CVE-2023-20198)
<https://www.fortiguard.com/threat-signal-report/5293>

Oct 19, 2023: CISA added CVE-2023-20198 to its known exploited list (KEV) Catalog.
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Latest Developments Oct 20, 2023: Cisco identified an additional vulnerability (CVE-2023-20273) that is exploited to deploy the implant. Fixes for both CVE-2023-20198 and CVE-2023-20273 are estimated to be available on October 22 according to the vendor advisory. Please see the following link for software fix availability:
<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>


PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Lure


Detects attack attempts related to Cisco IOS XE Web Attack and prevents lateral movement on the network segment



FortiDeceptor
v3.3+

Decoy VM

Detects attack attempts related to Cisco IOS XE Web Attack and prevents lateral movement on the network segment



FortiDeceptor
v3.3+






Weaponization

Delivery

Exploitation

IPS



Detects and blocks attack targeting the backdoor traffic on the vulnerable devices.

FortiGate DB 25.661 **FortiSASE** DB 25.661 **FortiNDR** DB 25.661 **FortiADC** DB 25.661 **FortiProxy** DB 25.661

Web App Security

Detects and blocks attacks related to Cisco IOS XE Web UI Attack

FortiWeb DB 0.00361 **FortiADC** DB 1.00046

Installation


C2

Action

DETECT


Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection




FortiAnalyzer
DB 2.00023

Threat Hunting



FortiAnalyzer
v6.4+

Content Update



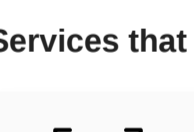
FortiSIEM
v6.6+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response



Services that can automatically respond to this outbreak.



FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

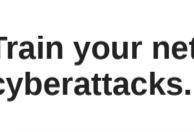
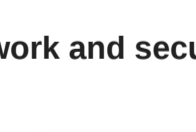
Incident Response **FortiRecon: ACI**

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

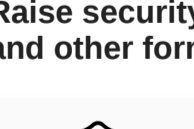
Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training **Response Readiness**

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.




Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening


Check Security Fabric devices to build actionable configuration recommendations and key indicators.



Security Rating

Business Reputation

Know attackers next move to protect against your business branding.



FortiRecon: EASM

Additional Resources

- Dark Reading** <https://www.darkreading.com/vulnerabilities-threats/critical-unpatched-cisco-zero-day-bug-active-exploit>
- Security Week** <https://www.securityweek.com/ens-of-thousands-of-cisco-devices-hacked-via-zero-day-vulnerability/>
- Security Week** <https://www.securityweek.com/number-of-cisco-devices-hacked-via-unpatched-vulnerability-increases-to-40000/>
- Cisco** <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>

Learn more about [FortiGuard Outbreak Alerts](#)