

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. Cisco IOS XE is the internetworking operating system used by the Next-Generation Cisco Systems such as routers

telecommunications providers as part of a cyber espionage campaign.

According to the vendor report, this vulnerability (CVE-2023-20198) allows a remote, unauthenticated attacker to

Background

and switches. The Web User Interface (WebUI) provides simplified deployment and manageability of the devices.

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. June 24, 2025: The Canadian Centre for Cyber Security and the U.S. Federal Bureau of Investigation (FBI) have

Latest Developments

https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-<u>global-cyberespionage-campaign</u> October 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

issued an advisory warning of cyber attacks mounted by the China-linked Salt Typhoon actors to breach major global

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-forcisco-ios.html

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

October 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

https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/ October 16, 2023: FortiGuard Labs released a Threat Signal for the vulnerability (CVE-2023-20198) https://www.fortiguard.com/threat-signal-report/5293

October 16, 2023: Cisco Talos released a detailed blog about the CVE-2023-20198 vulnerability and its active

PROTECT



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

exploitation.

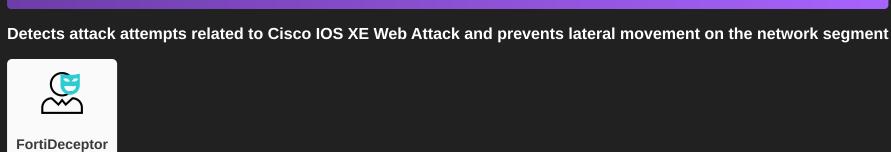
Detects attack attempts related to Cisco IOS XE Web Attack and prevents lateral movement on the network segment

FortiDeceptor

v3.3+

Decoy VM

Lure



v3.3+

Detects known malware related to the Outbreak

AV

FortiADC FortiCASB FortiCWP

v6.6+



FortiSASE

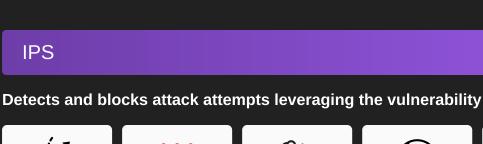
v6.6+

DB 25.661



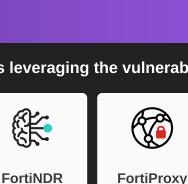
FortiGate

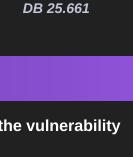
DB 25.661



v6.6+

DB 25.661





FortiClient

v6.6+

FortiGate

v6.6+

FortiMail

v6.6+

FortiProxy

v6.6+



DB 25.661

DB 1.00046

DB 0.00361



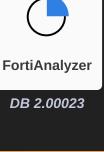
FortiADC



FortiWeb

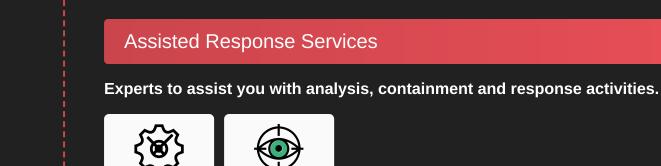
Outbreak Detection

IOC



Threat Hunting

v6.4+



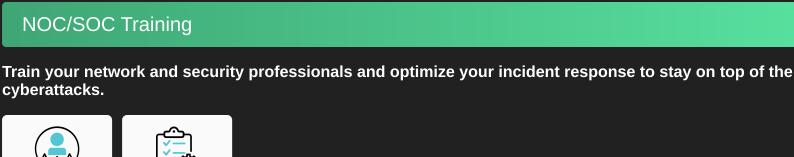
FortiXDR

RESPOND

Automated Response

Improve security posture and processes by implementing security awareness and training, in preparation for

Develop containment techniques to mitigate impacts of security events:



Response Readiness

Security **Awareness &**

Identify processes and assets that need protection: Attack Surface Hardening

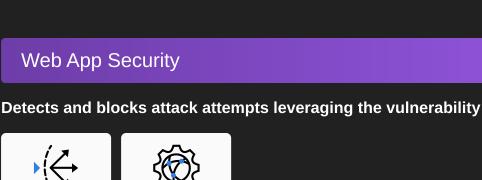
IDENTIFY

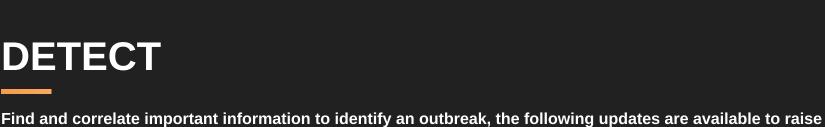
Know attackers next move to protect against your business branding.



FortiRecon:

IPS FortiADC

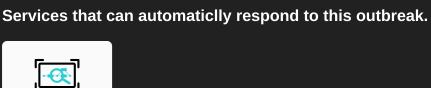




alert and generate reports:

FortiAnalyzer FortiSOCaaS FortiSIEM FortiSOAR

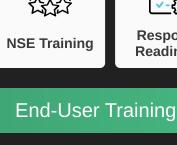




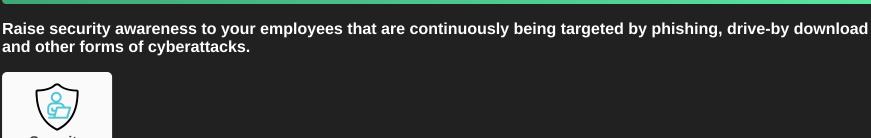
Response

RECOVER

(and recovery from) security incidents:



Training



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

Security Rating

Business Reputation



Dark Reading

Security Week

Security Week

https://www.darkreading.com/vulnerabilities-threats/critical-unpatched-cisco-zero-day-bug-active-exploit https://www.securityweek.com/tens-of-thousands-of-cisco-devices-hacked-via-zero-day-vulnerability/

Cisco https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-dublin-17121/221128-software-fix-availability-forcisco-ios.html

https://www.securityweek.com/number-of-cisco-devices-hacked-via-unpatched-vulnerability-increases-to-40000/

Learn more about FortiGuard Outbreak Alerts

F**I**RTINET.