SEQURETEK

Zero-day Vulnerability in Cisco IOS XE

OVERVIEW

Cisco disclosed a new high-severity zero-day vulnerability (CVE-2023-20273) that is actively being exploited to deploy malicious implants on IOS XE devices.

KNOWLEDGE BASE REGISTER

- Version Control

Issue Date	Version	Prepared by	Approved by
23 OCT 2023	v 1.0	Sindhuja Bidurukunta	Cdr. Subhash Dutta

OVERVIEW

- Cisco recently disclosed a new high severity vulnerability which affects Web UI feature of Cisco IOS XE devices.
- This newly identified flaw tracked as CVE-2023-20273, is actively being exploited to deploy malicious implants on IOS XE devices.
- This vulnerability is linked with another zero-day vulnerability (CVE-2023-20198) that was disclosed earlier by Cisco. The advisory updates the guidance given earlier in SQTK_ADV_2023_0051 – Vulnerability in Cisco IOS XE.
- According to Cisco, fixes for both CVE-2023-20198 and CVE-2023-20273 are now available.

IMPACT

- This flaw could allow the attacker to steal data, disrupt operations, or even launch attacks against other devices on the network.

AFFECTED PRODUCTS & VERSIONS

- Cisco IOS XE Software if the web UI feature is enabled.

TECHNICAL DETAILS

- When Cisco IOS XE software is exposed to the internet or untrusted networks, a previously undiscovered vulnerability in the Web User Interface (Web UI) feature (CVE-2023-20198) is actively being exploited, according to Cisco.
- This impacts Cisco IOS XE-running physical and virtual devices that have the HTTP or HTTPS Server feature enabled.
- Exploitation of this vulnerability allows an actor to gain full administrative privileges and unauthorized access into affected systems.
- Next, by taking advantage of a different web UI feature, the attacker was able to exploit new vulnerability.
- This new issue has been assigned CVE-2023-20273 by Cisco with CVSS Score of 7.2.
- After compromising the device through CVE-2023-20198, attackers don't stop there.
- They utilize another vulnerability in the Web UI feature, allowing them to install a malicious implant.
- This implant grants the attacker the ability to execute any command with root privileges, solidifying their control over the device.

- With such control, the attacker writes the implant to the system and this could allow the attacker to steal data, disrupt operations, or even launch attacks against other devices on the network.
- One method to identify if the implant is present is to run the following command against the device, where the "DEVICEIP" portion is a placeholder for the IP address of the device to check:

  curl -k -X POST "https[:]//DEVICEIP/webui/logoutconfirm.html?logon_hash=1"

CVE DETAILS

CVE-ID	CVSS Score	Severity	Vector
CVE-2023-20198	10.0	Critical	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- The attacker first exploited CVE-2023-20198 to gain initial access and issued a privilege 15 command to create a local user and password combination. This allowed the user to log in with normal user access.

CVE DETAILS

CVE-ID	CVSS Score	Severity	Vector
CVE-2023-20273	7.2	High	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

- After that, the attacker took advantage of another web UI feature, using the newly created local user to elevate privileges to root and write the implant to the file system. This issue is known by Cisco as CVE-2023-20273.

FIXED VERSIONS

Cisco IOS XE Software Release Train	First Fixed Release
17.9	17.9.4a
17.6	17.6.6a
17.3	17.3.8a
16.12 (Catalyst 3650 and 3850 only)	16.12.10a

INDICATORS of COMPROMISE

IoCs are tabulated in the accompanying document to this advisory (Doc Ref SQTK advisory- SQTK_ADV_2023_0053-Zero-day Vulnerability in Cisco IOS XE-IoCs.pdf).

CORRECTIVE & PREVENTIVE ACTIONS

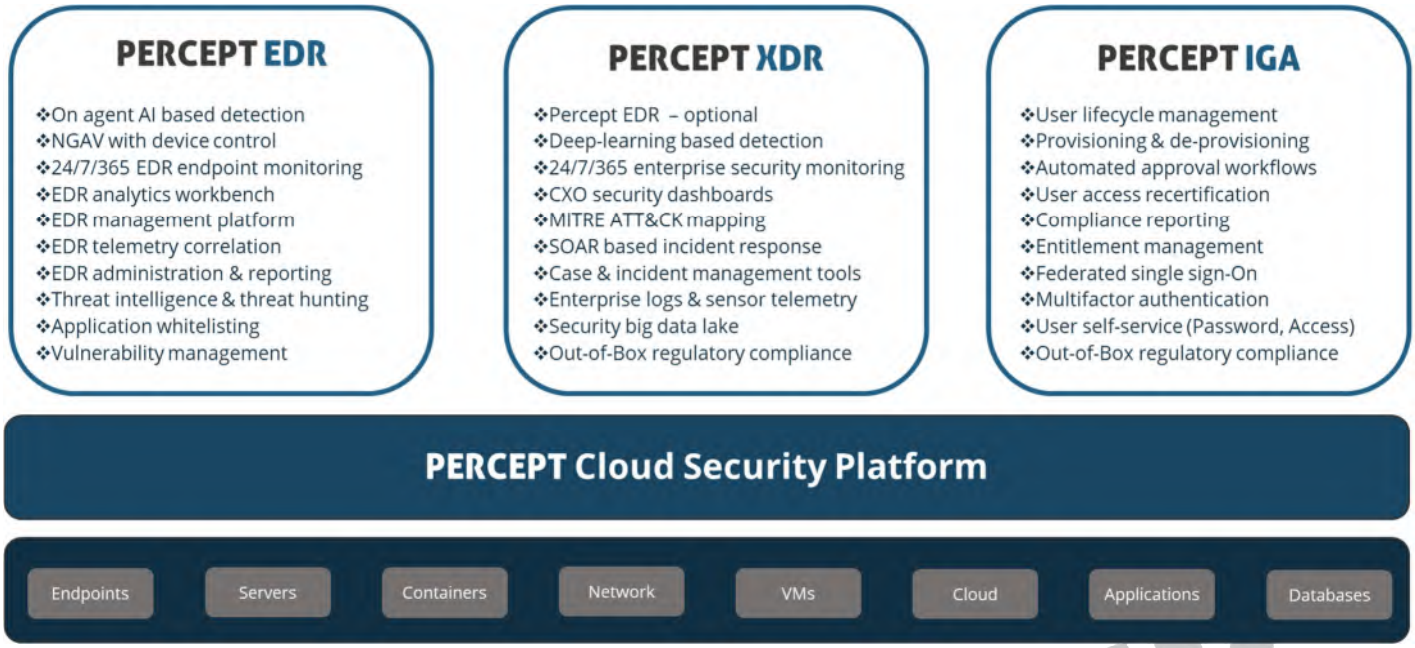
- Upgrade to a Fixed Version.
- If you are unable to apply the fix immediately, Cisco recommends that you disable the vulnerable HTTP server feature on all internet-facing systems.
- Should also look for suspicious or recently created user accounts as potential indicators of malicious activity associated with these ongoing attacks.
- To disable the HTTP Server feature, use the *no Ip http* server or *no Ip http* secure-server command in global configuration mode.
- If both the HTTP server and HXXPS server are in use, both commands are required to disable the HTTP Server feature.

REFERENCES

[1].hxxps://sec.cloudapps[.]cisco[.]com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
[2].hxxps://blog[.]talosintelligence[.]com/active-exploitation-of-cisco-ios-xe-software/
[3].hxxps://securityonline[.]info/cve-2023-20273-cisco-ios-xe-zero-day-vulnerability/?expand_article=1
[4].hxxps://gixtools[.]net/2023/10/multiple-vulnerabilities-in-cisco-ios-xe-software-web-ui-feature/
[5].hxxps://www[.]tenable[.]com/cve/CVE-2023-20273

About Sequretek

Sequretek is a global cybersecurity company which offers end-to-end security in the areas of enterprise threat monitoring, incident response, device security, identity & access governance through our own AI driven Percept Cloud Security Platform.



Take Control of your enterprise security

- Enterprise scale, easy to use and cloud native
- AI driven threat detection, protection, remediation and response
- Quick implementation and integration capabilities
- End-to-End ownership and management of Sequretek products
- Reduce Total Cost of Ownership (TCO) while simplifying security

Feel free to reach out at info@sequretek[.]com to know more about our productsor schedule a demo at hxxps[:]//sequretek[.]com/request-a-demo/