SEQURETEK

Vulnerability in Cisco IOS XE

OVERVIEW

A vulnerability in Cisco IOS XE enables a remote attacker to take over the system.

KNOWLEDGE BASE REGISTER

- Version Control

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

OVERVIEW

- Cisco has released an advisory regarding exploitation of a previously unknown vulnerability (CVE-2023-20198) in the web UI feature of Cisco IOS XE Software.
- The zero-day vulnerability allows a remote unauthenticated attacker to create an account on an affected system with privilege level 15 access, which is the highest level of access that allows an attacker to gain complete control over the vulnerable system.
- However, according to Cisco, there is no patch available presently. Cisco has released guidance to address this vulnerability.

IMPACT

- The attacker can create accounts on the vulnerable system that can be used for further compromise of the environment.

AFFECTED SOFTWARES & VERSIONS

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

TECHNICAL DETAILS

- A vulnerability in the web UI feature of Cisco IOS XE Software, when exposed to the internet or to untrusted networks, could allow an unauthenticated, remote attacker to create an account on an affected system with privilege level 15 access.
- In Cisco IOS, privilege level 15 provides complete control over a device.
- This includes: Entering Privileged Exec mode, full access to all commands, including the *Reload* command.
- The attacker can then use that account to gain control of the affected system.
- The disclosure reported that the vulnerability had been exploited in the wild to help install implants on affected switches and routers.
- Cisco also provided a straightforward method to check if an IOS XE device had an active implant installed on it. When a particular HTTP POST is sent to the system, the implant replies with an 18-character hexadecimal string:

```
$ curl -X POST http://192.168.1.1/webui/logoutconfirm.html?logon_hash=1
1a80b7389ccd0a5dab
```

- Attackers can use CVE-2023-20198 to create persistent local user accounts that grant them continued administrator-level access on vulnerable systems even after a device restart.
- Researchers from Cisco urged companies to keep an eye out for new or strange users on IOS XE devices as these could be signs that attackers have taken advantage of the vulnerability.

INDICATORS of COMPROMISE

IoCs are tabulated in the accompanying document to this advisory (Doc Ref SQTK_ADV_2023_0051- Vulnerability in Cisco IOS XE.pdf).

CORRECTIVE & PREVENTIVE ACTIONS

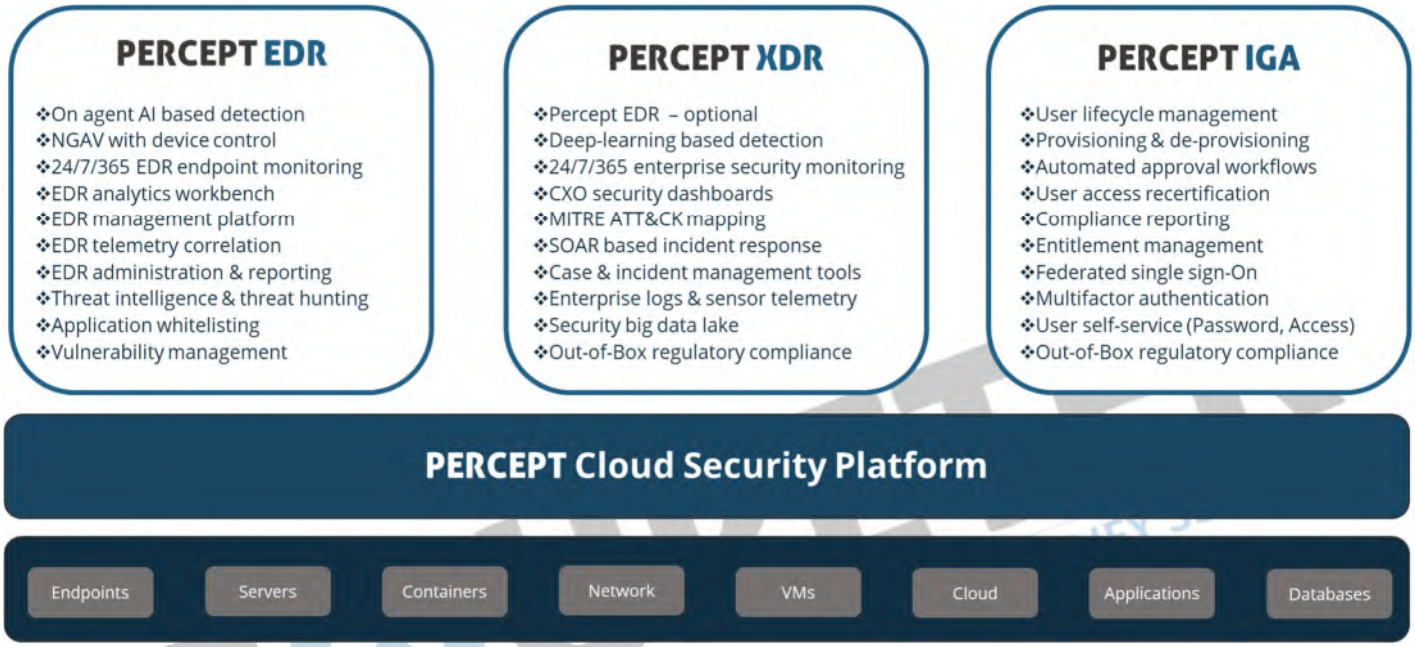
- Protect your organization by disabling the web interface and removing all management interfaces from the internet immediately.
- Cisco strongly recommends that customers disable the HTTP Server feature on all internet-facing systems.
- To disable the HTTP Server feature, use the *no Ip http server* 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.
- Apply the patch when released by Cisco.

REFERENCES

[1].hxxps://blog.talosintelligence[.]com/active-exploitation-of-cisco-ios-xe-software/
[2].hxxps://www[.]cisecurity[.]org/advisory/a-vulnerability-in-cisco-ios-xe-software-web-ui-could-allow-for-privilege-escalation_2023-122
[3].hxxps://www[.]systemtek[.]co.uk/2023/10/cisco-ios-xe-software-web-ui-privilege-escalation-vulnerability-cve-2023-20198/
[4].hxxps://www[.]lansweeper[.]com/vulnerability/critical-zero-day-in-cisco-ios-xe-could-lead-to-privilege-escalation/
[5].hxxps://www[.]cvedetails[.]com/cve/CVE-2023-20198/
[6].hxxps://sec[.]cloudapps[.]cisco[.]com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

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/