FINISHED INTELLIGENCE REPORTS

Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities

TLP:WHITE

Nov 01, 2023

On November 01, 2023, CISA released Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities. The guidance now notes that Cisco has fixed these vulnerabilities for the 17.3 Cisco IOS XE software release train with version 17.3.8a. Health-ISAC is distributing this report for your situational awareness.

Widespread exploitation of two vulnerabilities, CVE-2023-20198 and CVE-2023-20273, affecting Cisco's Internetworking Operating System (IOS) XE Software Web User Interface (UI). Cisco's IOS XE Web UI is a system management tool for IOS XE, which is a network operating system for use on various Cisco products. An unauthenticated remote actor could exploit these vulnerabilities to take control of an affected system. Specifically, these vulnerabilities allow the actor to create a privileged account that provides complete control over the device.

Organizations running IOS XE Web UI should immediately implement the mitigations outlined in Cisco's Security Advisory, Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature, which include disabling the HTTP Server feature on internet-facing systems, and hunt for malicious activity on their network. According to the Cisco Talos blog, Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerabilities, Organizations should look for unexplained or newly created users on devices as evidence of

potentially malicious activity relating to this threat. See the Talos blog for specific detection methods.

CVE-2023-20198 is a privilege escalation vulnerability in the web UI feature of Cisco's IOS XE software affecting both 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. After obtaining the privileged account, the actor can then create a local user account with normal privileges to exploit another IOS XE Web UI vulnerability, CVE-2023-20273—a command Injection vulnerability—to inject commands with elevated (root) privileges, enabling the actor to run arbitrary commands on the device.

According to the Cisco Talos blog referenced above, a threat actor can:

- Exploit CVE-2023-20198 to obtain initial access and create a privileged account.
- Use the privileged account to create a local user account with normal privileges.
- Using the local user account, exploit another Cisco IOS XE Web UI vulnerability—CVE-2023-20273—to inject commands with elevated (root) privileges, which enables the actor to run arbitrary commands on the device.

Actions for Organizations Running Cisco IOS XE Web UI

CISA urges organizations running Cisco IOS XE Web UI to immediately implement the mitigations outlined in Cisco's Security Advisory, which include disabling the HTTP Server feature on internet-facing systems, and hunt for malicious activity on their network.

Reference(s)	Cisco, Cisco, Cisco Talos, Cisco

Release Date

Nov 02, 2023 (UTC)

Alert ID 501d0b6a

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments

Please email us at contact@h-isac.org

Share Threat Intel

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Knowledge Base

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

CISA CISA is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.

Access the Health-ISAC Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

Download Health-ISAC’s Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**