TLP:CLEAR

U.S. COAST GUARD

MARITIME CYBER BULLETIN

20 October 2023

Critical Cisco IOS XE Software Web User Interface (UI) Privilege Escalation Vulnerability Identified

THREAT SUMMARY

Users of Cisco's IOS XE software could be vulnerable to a previously unknown exploitation when the software's web user interface (UI) feature is enabled and exposed to the internet or to untrusted networks. This vulnerability allows an attacker to create an account with the highest access privilege, level 15, and remotely gain control of the affected system through unauthenticated means. Cisco rates this vulnerability as **CRITICAL**.

Recommendations

There are currently no workarounds, but Cisco "Strongly recommends that customers disable the Hyper Text Transfer Protocol (HTTP) server feature on all internet facing systems."

For those using Cisco products and software with the web UI feature enabled, please refer to the following references for further guidance:

- Cisco's Security Advisory *Cisco IOS XE Software Web UI Privilege Escalation*
- Vulnerability Advisory ID *cisco-sa-iosxe-webui-privesc-j22SaA4z*

Resources

Facilities that observe any unusual activity or interruptions to their network should report those activities per CG-5P Policy Letter 08-16 – Reporting Suspicious Activity and Breaches of Security to:

- Coast Guard's National Response Center **1-800-424-8802**

OR

- Cybersecurity and Infrastructure Security Agency (CISA) Central **1-888-282-0870**

If you have any questions, please visit our website at: https://www.uscg.mil/MaritimeCyber or reach out to the Maritime Cyber Readiness Branch (MCRB) at: maritimecyber@uscg.mil

SOURCES

"Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature." 2023. October 20, 2023. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z.

The information contained in this bulletin is provided for **informational purposes only**. This information is based on common standards and best practices, the implementation of which does not relieve any domestic, international safety, operational, or material requirements. The USCG does not provide any warranties of any kind regarding this information and shall not be held liable for any damages of any kind that arose out of the results of, or reliance upon this information. Information Sharing Protocol: (https://www.us-cert.gov/tlp)