Cisco IOS XE Escalation of Privilege Vulnerability

Severity Level: High

Components Affected

- Cisco IOS XE

Overview

A vulnerability was identified in Cisco IOS XE. A remote attacker could exploit this vulnerability to trigger elevation of privilege on the targeted system.

Description

The primary vulnerability is the Elevation of Privilege which has been identified and tracked under CVE-2023-20198.This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access. The attacker can then use that account to gain control of the affected system.

Impact

- Elevation of Privilege

Solution/ Workarounds

Cisco recommends to 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 HTTPS server are in use, both commands are required to disable the HTTP Server feature.

Reference

- https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerability_20230912
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.