Security Advisory 2025-010

Critical Vulnerability in Cisco IOS XR Software

2025-03-14 — v1.0

TLP:CLEAR

History:

- *14/03/2025 — v1.0 – Initial publication*

Summary

On March 13, 2025, CISCO released an advisory regarding a critical vulnerability identified in Cisco's IOS XR Software [1].

It is recommended updating affected assets as soon as possible.

Technical Details

The vulnerability **CVE-2025-20138**, with a CVSS score of 8.8, stems from insufficient input validation in specific CLI (Command Line Interface) commands within the 64-bit version of Cisco IOS XR Software. Attackers can exploit this by crafting malicious arguments that escalate their privileges to root level. This enables full control over the device, potentially leading to unauthorised command execution, data manipulation, or system destabilisation [2].

Affected Products

The following Cisco IOS XR 64-bit Software versions are affected by the vulnerability:

- 24.1 and earlier
- 24.2 before 24.2.21
- 24.3

Recommendations

CERT-EU recommends updating the affected products as soon as possible to the latest version.

Detection

To identify if this vulnerability has been exploited, monitor system logs for any unauthorised root-level command executions.

References

[1] https://cybersecuritynews.com/cisco-ios-xr-software-vulnerability-command/

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-priv-esc-GFQjxvOF