Date Posted: 2026/03/19

[Vulnerability Alert] 2 Critical Security Vulnerabilities Found in Cisco IOS XR Software

- Subject Explanation: [Vulnerability Alert] 2 Critical Security Vulnerabilities Found in Cisco IOS XR Software

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202603-00000013
  - Recently, Cisco released a critical security advisory for IOS XR Software (CVE-2026-20040, CVSS: 8.8 and CVE-2026-20046, CVSS: 8.8). Both are CLI privilege escalation vulnerabilities. CVE-2026-20040 could allow an authenticated local attacker to execute arbitrary commands as root on the underlying operating system of the affected device; CVE-2026-20046 exists in the task group assignment of specific CLI commands, which could allow an authenticated local attacker to escalate privileges and gain full administrative control of the affected device.
- Impacted Platforms:
  - Cisco IOS XR Software versions 25.1 and earlier
  - Cisco IOS XR Software version 25.2
  - Cisco IOS XR Software version 25.3
  - Cisco IOS XR Software version 25.4
- Suggested Measures:
  - Please update to the following versions:
  - [CVE-2026-20040] Cisco IOS XR Software version 25.2.21, Cisco IOS XR Software version 25.4.2
  - Note: For Cisco IOS XR Software versions 25.1 and earlier, and version 25.3, please migrate to a fixed release.
  - [CVE-2026-20046] Cisco IOS XR Software version 25.2.2
  - Note: For Cisco IOS XR Software versions 25.1 and earlier, please migrate to a fixed release.
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10780-6b3d3-1.html

Computer and Communication Center
Network Systems Division