Health-ISAC®
Collaborating for Resilience in Health

Cisco Patches Two High-Severity Flaws in IOS XR software (CVE-2026-20040, CVE-2026-20046)

Mar 13, 2026
○ WHITE

View Alert

On March 11, 2026, Cisco released an advisory for IOS XR software, addressing two high-severity vulnerabilities, CVE-2026-20040 and CVE-2026-20046, which allow authenticated users to gain root and administrative access.

Additional Info

Analysis

These flaws, tracked as CVE-2026-20040 and CVE-2026-20046, involve improper CLI command validation and incorrect task group mapping. In the event of a successful attack, the flaws could allow unprivileged attackers to elevate their privileges to root or administrator, granting them total control over the underlying operating system.

Because these vulnerabilities bypass standard authorization checks, an internal actor or a compromised low-level account could execute arbitrary commands and modify system configurations without detection.

While Cisco has not observed these flaws being weaponized in the wild, the potential for attackers to disrupt regional telecommunications or gain root access makes these patches essential to maintaining network integrity.

To protect your infrastructure, immediately upgrade to the latest patched release of Cisco IOS XR as specified in the advisory.

Affected products

- CVE-2026-20040 affects Cisco IOS XR Software across all device configurations.
- CVE-2026-20046 impacts Cisco IOS XRv 9000 Routers, regardless of configuration.

Recommendations

- Immediately apply updates for the affected Cisco devices.
- Segment networks and implement strict network access controls.
- Continuously monitor logs for suspicious activity.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

<hr size=1 width="100%" align=center>

Alert Id	0808ea8c
Category	Vulnerability Bulletins
Tags	CVE-2026-20046, CVE-2026-20040, IOS XR Software, Cisco

Sources

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-privesc-bF8D5U4W
https://securityonline.info/root-access-via-cli-cisco-patches-critical-ios-xr-privilege-escalation-flaws/
https://cybersecuritynews.com/cisco-ios-xr-software-vulnerability-root/

Incident Date

Mar 12, 2026 (UTC)

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

Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App

Available on iOS, Android and Web

Download on the App Store Get it on Google Play

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/0100019ce78f5621-08d67bf0-0e02-4865-af83-f595eb3ade32-000000%40email.amazonses.com.