**GOVERNMENT OF THE REPUBLIC OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

**GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

3 September 2026

## Advisory 247: Cisco IOS XR Software Improper Control of a Resource Through Its Lifetime (CVE-2026-20274).

**Release Date:** 2nd September 2026
**Impact:** CRITICAL
**TLP:** CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, System/Network administrators, and telecommunications/Internet Service Provider network engineering teams that deploy or operate Cisco IOS XR Software on carrier-grade routing platforms. This alert is intended to be understood by technical users and systems administrators.

# What is it?

CVE-2026-20274 is a critical vulnerability in Cisco IOS XR Software, Cisco's carrier-grade network operating system used on service-provider and enterprise core/edge routing platforms (including the ASR 9000 Series and other Cisco IOS XR-based routers), rooted in improper control of a resource through its lifetime. The vulnerability affects all releases of Cisco IOS XR Software, including Cisco IOS XR7 (LNT) Software, regardless of device configuration. It was identified by Cisco's own IOS XR engineering team as part of a comprehensive internal security review, and disclosed together with six related CVEs - including CVE-2026-20279 (covered separately in CERTVU Advisory 246) in the same Cisco IOS XR Software Security Hardening Release for September 2026; this advisory covers CVE-2026-20274 specifically, and organizations remediating it should be aware the same hardening release addresses the other six CVEs as well, using the same fixed-release table.

# What are the systems affected?

The following version(s) are affected:

- All releases of Cisco IOS XR Software, including Cisco IOS XR7 (LNT) Software, regardless of device configuration – (Affected)

Cisco has not released a single unified "fixed version" for this vulnerability - instead, fixes are delivered per software train as Security Maintenance Updates (SMUs) that must be applied on top of the existing release (for example, SMUs are available for 6.9.2, 7.3.2, 24.4.2, and 26.1.2, among other trains; some trains, such as 26.3, receive their fix directly in the upcoming 26.3.1 release). This is the same fixed-release table that applies to CVE-2026-20279/Advisory 246 and the other CVEs in the same hardening release. Cisco states that future Cisco IOS XR Software releases 26.2.2 and 26.3.1 will be the first fixed releases that do not require a separate SMU. Because the exact required SMU or fixed release depends on which train a given device is running, administrators should consult the fixed-release table in Cisco Security Advisory cisco-sa-hardening-iosxr-qg64NcM directly, or use Cisco's Software Checker tool, rather than relying on a single version number.

# What does this mean?

**Typical attack flow:**

1. **Reach the affected resource-handling function on an exposed IOS XR device**
    - An attacker sends a crafted request or input to a reachable Cisco IOS XR device — Cisco's advisory does not publish the specific vulnerable interface, protocol, or memory-handling routine to avoid providing an exploitation roadmap, describing the underlying issue only in general terms as improper control of a resource through its lifetime, a category covering memory-safety issues such as buffer overflows and use-after-free conditions.
2. **Corrupt device memory or resource state to achieve compromise**
    - Because no authentication or user interaction is required (CVSS AV:N/AC:L/PR:N/UI:N), a successful attacker can corrupt the affected resource's state or memory, with the potential for complete compromise of the device's confidentiality, integrity, and availability — up to and including a device crash/reload (denial of service) or arbitrary code execution, depending on which specific underlying weakness is present.

# Mitigation process

CERTVU recommends the following:

1. Apply the appropriate Security Maintenance Update (SMU) or fixed release without delay, since Cisco has stated there is no workaround

- Identify the exact IOS XR software train running on each device and apply the corresponding SMU listed in Cisco Security Advisory cisco-sa-hardening-iosxr-qg64NcM (or use Cisco's Software Checker tool), or upgrade to a fixed release such as the upcoming 26.2.2 or 26.3.1 once available. This is the same remediation path as CVE-2026-20279/Advisory 246 - one SMU/upgrade addresses both.

2. Since Cisco has confirmed there are no workarounds for this vulnerability, prioritize the SMU/patch rollout over any temporary compensating control
3. Audit the estate for Cisco IOS XR deployments
4. Treat any internet-reachable, unpatched device as potentially compromised
5. Review device stability and configuration

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

# Reference


1. https://www.cve.org/CVERecord?id=CVE-2026-20274
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxr-qg64NcM