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 248: Cisco Nexus 9000 Series Silicon One Remote Code Execution (CVE-2026-20212).

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 data centre network engineering teams that deploy or operate Cisco Nexus 9000 Series Switches. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-20212 is a critical remote code execution vulnerability in the Silicon One ASIC integration used by certain Cisco Nexus 9000 Series Switches - high-performance data centre switching platforms. TCP ports 43210 and 43211, used by the Silicon One Hardware Abstraction Layer (S1HAL) process, are accessible in the default Layer 3 VRF (Virtual Routing and Forwarding instance). An unauthenticated, remote attacker who can reach these ports can send crafted input that is executed with root privileges on the device, or that crashes the S1HAL process and triggers a device reload. This vulnerability was found internally by Cisco during the resolution of a Cisco Technical Assistance Center (TAC) support case, not reported by an external researcher.

What are the systems affected?

The following version(s) are affected:

- Cisco Nexus 9000 Series Switches equipped with a Silicon One ASIC, including models N9324C-SE1U, N9348Y2C6D-SE1U, N9364E-SG2-O, N9364E-SG2-Q, N9396T12C-SE1, N9348Y12C-SE1, N9396Y12C-SE1, N9336C-SE1, N9K-C9804, and N9K-C9808 – (Affected)

Cisco's advisory does not publish a single fixed-release table; instead, it directs customers to Cisco's own Software Checker tool to identify the correct fixed NX-OS release for their specific platform and current version. Nexus 9000 switches that do not include a Silicon One ASIC (the majority of the Nexus 9000 line) are not affected by this specific CVE.

What does this mean?

Typical attack flow:

1. **Reach TCP port 43210 or 43211 on an affected switch**
    - An unauthenticated attacker with network access to an affected Nexus 9000 switch's default Layer 3 VRF connects to TCP port 43210 or 43211, both used by the Silicon One Hardware Abstraction Layer (S1HAL) process and reachable without any access restriction by default.
2. **Send crafted input to execute code as root, or crash the S1HAL process**
    - The attacker sends crafted input to the exposed port, which the S1HAL process executes with root privileges — or, alternatively, the crafted input crashes the S1HAL process, triggering a reload of the switch and a denial-of-service condition.

Mitigation process

CERTVU recommends the following:

1. Apply the workaround immediately, then upgrade to a fixed release

- Use infrastructure access control lists (iACLs) to allow only required management and control-plane traffic to the device, or to explicitly deny TCP packets destined to a locally-configured IP address on port 43210 or 43211 (per Cisco's own published workaround). Cisco has also released a "Live Protect shield" for CVE-2026-20212 as a temporary mitigation. Use Cisco's Software Checker tool to identify and apply the correct fixed NX-OS release for your platform as the permanent remediation.

2. Prioritize this workaround and patch on every affected switch, since unauthenticated root-level code execution is the most severe practical outcome a network device vulnerability can have
3. Audit the estate for affected Nexus 9000 hardware
4. Treat any internet-reachable, unmitigated switch 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-2026-20212

2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9k-s1-rce-EH8dEtr