

**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

2 September 2026

Advisory 229: HPE Aruba Networking AOS-CX Unauthenticated Remote Code Execution Vulnerability (CVE-2026-73749).

Release Date: 1st 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 and System/Network administrators that operate switches running HPE Aruba Networking AOS-CX, the switch operating system used across many enterprise and campus network deployments. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-73749 (CVSS 3.1 base score 9.8, Critical) affects a network-facing daemon in HPE Aruba Networking AOS-CX that improperly processes malformed input. An unauthenticated remote attacker can send specially crafted packets to the affected service, with no privileges or user interaction required, resulting in remote code execution with elevated privileges on the switch.

CVE-2026-73749 was disclosed on 1 September 2026 alongside related AOS-CX vulnerabilities (including CVE-2026-73782 and CVE-2026-73783) in the same HPE security bulletin; this advisory covers CVE-2026-73749 specifically. Because AOS-CX runs the core switching and routing function of the network devices it operates on, remote code execution at elevated privilege on an affected switch can expose the traffic and segments that switch carries, not just the device itself.

What are the systems affected?

The following version(s) are affected:

- HPE Aruba Networking AOS-CX 10.18.0000, 10.17.0000, 10.16.0000, 10.13.0000, and 10.10.0000 trains (and earlier builds within each train) – (Affected)

See HPE Security Bulletin HPESBNW05134 for the specific fixed build on each AOS-CX train – (Not affected, patched)

CERTVU verify that HPE's public bulletin (docId HPESBNW05134) is the authoritative source for the exact fixed build number on each affected AOS-CX train. Patching is critical.

What does this mean?

Typical attack flow:

1. **Reach the affected AOS-CX daemon**
 - An attacker identifies a switch running an affected HPE Aruba Networking AOS-CX build with the vulnerable daemon reachable over the network.
2. **Send malformed input to trigger remote code execution**
 - The attacker sends specially crafted packets that the daemon fails to process correctly, triggering remote code execution with elevated privileges on the switch, with no authentication or user interaction required.

Attack vectors:

- Direct network access to the affected AOS-CX daemon on the switch — no authentication, prior access, or user interaction is required.
- Particular risk where AOS-CX switch management or service interfaces are reachable from outside a trusted management network or the internet.

Successful exploitation may allow attackers to:

- Execute arbitrary code with elevated privileges on the affected switch.
- Gain control of a core network device, with potential impact on the confidentiality, integrity, and availability of every network segment that switch carries.

Mitigation process

CERTVU recommends the following:

1. Apply the HPE fix without delay

- Consult HPE Security Bulletin HPESBNW05134 for the specific fixed build for each affected AOS-CX train and apply it as a priority, given the maximum CVSS score and lack of any exploitation precondition.

2. Restrict network exposure of AOS-CX management and service interfaces
3. Segment and monitor switch management traffic pending patching
4. Audit the estate for the affected product
5. Conduct a compromise assessment

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

Reference

1. https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05134en_us&docLocale=en_US
2. <https://www.cve.org/CVERecord?id=CVE-2026-73749>