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 230: HPE Aruba Networking Fabric Composer API Authentication Bypass Vulnerability (CVE-2026-76657).

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 and System/Network administrators that operate HPE Aruba Networking Fabric Composer (AFC) for managing data centre network fabrics. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-76657 is a maximum-severity vulnerability (CVSS 3.1 base score 10.0) in the API of HPE Aruba Networking Fabric Composer, caused by improper authentication (CWE-287). The flaw allows an unauthenticated remote attacker to circumvent existing authentication controls on the AFC API and gain administrative access to the underlying host, with no privileges and no user interaction required.

CVE-2026-76657 was disclosed on 1 September 2026 in the same HPE security bulletin as CVE-2026-76658, an SSH daemon authentication bypass in the same product that CERTVU addressed in Advisory 226. The two are companion, separately exploitable flaws in different AFC interfaces (API versus SSH daemon) rather than the same bug. As with the SSH-daemon flaw, an attacker who obtains administrative access to the AFC host can execute arbitrary operating-system commands as a privileged user, resulting in complete compromise of the management platform and placing every network fabric it administers at risk. Patching is critical.

What are the systems affected?

The following version(s) are affected:

- HPE Aruba Networking Fabric Composer 7.0.0 – (Affected)

See HPE Security Bulletin HPESBNW05133 for the fixed release and update package – (Not affected, patched)

CERTVU verify HPE's public bulletin (docId HPESBNW05133) is the authoritative source for the specific fixed version and download package, and covers both CVE-2026-76657 and CVE-2026-76658 together.

What does this mean?

Typical attack flow:

1. **Reach the AFC API**
    - An attacker identifies an HPE Aruba Networking Fabric Composer host with its API reachable over the network.
2. **Bypass authentication and gain administrative access**
    - The attacker sends crafted requests to the AFC API that circumvent existing authentication controls, obtaining administrative access without valid credentials, then executes arbitrary operating-system commands as a privileged user on the AFC host.

Attack vectors:

- Direct network access to the API service on an affected AFC host — no authentication, prior access, or user interaction is required.
- Particular risk where the AFC API or management interface is reachable from outside a trusted management network or the internet.

Successful exploitation may allow attackers to:

- Circumvent authentication on the AFC API and gain full administrative access to the AFC host.
- Achieve complete compromise of the network fabric management platform, with downstream risk to every switch fabric that AFC instance administers.

Mitigation process

CERTVU recommends the following:

1. Apply the HPE fix without delay

- Consult HPE Security Bulletin HPESBNW05133 for the specific fixed release and apply it to every affected Fabric Composer 7.0.0 instance as a priority, given the maximum CVSS score and lack of any exploitation precondition. If your organization has already patched for CVE-

2026-76658 (Advisory 226), confirm that same update also resolves CVE-2026-76657 rather than assuming it.

2. Restrict network exposure of the AFC API and management interface
3. Restrict administrative access 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=hpesbnw05133en_us&docLocale=en_US
2. https://www.cve.org/CVERecord?id=CVE-2026-76657