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 226: HPE Aruba Networking Fabric Composer SSH Authentication Bypass Vulnerability (CVE-2026-76658).

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 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-2026-76658 is a maximum-severity vulnerability (CVSS 3.1 base score 10.0) in the SSH daemon of HPE Aruba Networking Fabric Composer, caused by improper authentication (CWE-287). The flaw allows an unauthenticated remote attacker to gain administrative access to the underlying AFC host over the network, with no privileges and no user interaction required.

Because AFC is used to centrally manage and provision switch fabrics, 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. This vulnerability is currently being exploited in the wild, but the combination of maximum severity, network attack vector, and no authentication required makes this a priority patch for any site running the affected release.

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

What does this mean?

Typical attack flow:

1. **Reach the AFC management interface**
    - An attacker identifies an HPE Aruba Networking Fabric Composer host reachable over the network, including its SSH daemon.
2. **Bypass authentication and gain administrative access**
    - The attacker exploits the improper authentication flaw in the SSH daemon to obtain 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 SSH service on an affected AFC host - no authentication, prior access, or user interaction is required.
- Particular risk where the AFC management interface is reachable from outside a trusted management network or the internet.

Successful exploitation may allow attackers to:

- Gain full administrative access to the AFC host and execute arbitrary operating-system commands as a privileged user.
- 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.

2. Restrict network exposure of the AFC 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-2026-76658