

**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 232: HPE Aruba Networking Fabric Composer Unauthenticated Remote Code Execution Vulnerability (CVE-2026-73701).

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-2026-73701 (CVSS 3.1 base score 9.0, Critical) is an unauthenticated remote code execution vulnerability in the underlying operating system of HPE Aruba Networking Fabric Composer. No privileges or user interaction are required to exploit it, but HPE's description notes that exploitation depends on certain preconditions outside the attacker's control being met, which is reflected in the CVSS vector's High attack complexity rating rather than the Low complexity seen in the related SSH-daemon and API bypass flaws. HPE has not published further detail on what those preconditions are.

CVE-2026-73701 was disclosed on 1 September 2026 in the same HPE security bulletin as CVE-2026-76657, CVE-2026-76658, and CVE-2026-73700, three further critical vulnerabilities in the same product that CERTVU addressed in Advisory 230, Advisory 226, and Advisory 231 respectively. This is a distinct, fourth vulnerability rather than a duplicate of any of those. Successful exploitation results in arbitrary code execution as a privileged user on the underlying operating

system, leading to complete compromise of the AFC host, consistent with the other advisories in this bulletin.

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 CVE-2026-73701 alongside CVE-2026-76657, CVE-2026-76658, and CVE-2026-73700.

What does this mean?

Typical attack flow:

1. **Reach an affected AFC host under the right conditions**
 - An attacker identifies an HPE Aruba Networking Fabric Composer host reachable over the network, where the unspecified preconditions required for this flaw happen to be met.
2. **Achieve remote code execution on the underlying operating system**
 - The attacker exploits the underlying operating-system vulnerability to execute arbitrary code as a privileged user, with no authentication or user interaction required once the preconditions are satisfied.

Attack vectors:

- Network access to an affected AFC host — no authentication, prior access, or user interaction is required, though the flaw depends on preconditions outside the attacker's control that HPE has not detailed.
- Particular risk where the AFC host is reachable from outside a trusted management network or the internet, increasing the chance that any qualifying preconditions are met by an opportunistic attacker.

Successful exploitation may allow attackers to:

- Execute arbitrary code as a privileged user on the underlying operating system of 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. If your organization has already patched for CVE-2026-76657, CVE-2026-76658, or CVE-2026-73700 (Advisories 230, 226, and 231), confirm that same update also resolves CVE-2026-73701 rather than assuming it.

2. Restrict network exposure of the AFC host
3. Treat AFC as a high-value target 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-2026-73701>