

**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 233: HPE Aruba Networking Fabric Composer Authentication Bypass Vulnerability (CVE-2026-19766).

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-2026-19766 (CVSS 3.1 base score 9.6, Critical) is an authentication bypass vulnerability in the underlying operating system of HPE Aruba Networking Fabric Composer. Unlike the other flaws in this bulletin, this one requires the attacker to be on the adjacent network (CVSS attack vector "Adjacent" rather than "Network"), but otherwise requires no privileges and no user interaction, and has low attack complexity. Successful exploitation allows an unauthenticated adjacent attacker to execute arbitrary code as a privileged user on the underlying operating system, leading to complete compromise of the AFC host.

CVE-2026-19766 was disclosed on 1 September 2026 in the same HPE security bulletin (HPESBNW05133) as CVE-2026-76657, CVE-2026-76658, CVE-2026-73700, and CVE-2026-73701, four further critical vulnerabilities in the same product that CERTVU addressed in Advisory 230, Advisory 226, Advisory 231, and Advisory 232 respectively. This is a distinct, fifth 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, though this flaw specifically requires adjacent network access rather than being exploitable from anywhere on the network.

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-2026-19766 alongside CVE-2026-76657, CVE-2026-76658, CVE-2026-73700, and CVE-2026-73701.

What does this mean?

Typical attack flow:

1. **Gain adjacent network access to an affected AFC host**
 - An attacker positions themselves on the same local or adjacent network segment as an HPE Aruba Networking Fabric Composer host, for example by compromising another device on that segment or gaining access to the management network.
2. **Bypass authentication and execute code as a privileged user**
 - The attacker exploits the authentication bypass in the underlying operating system to execute arbitrary code as a privileged user, with no valid credentials, prior access, or user interaction required beyond adjacent network positioning.

Attack vectors:

- Adjacent network access to an affected AFC host — no authentication, prior access, or user interaction is required, but the attacker must be on the same local or adjacent network segment rather than able to reach the host from anywhere on the network.
- Particular risk in flat or poorly segmented network designs where an attacker who compromises any device on the same segment as the AFC host can reach it directly.

Successful exploitation may allow attackers to:

- Bypass authentication and 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, CVE-2026-73700, or CVE-2026-73701 (Advisories 230, 226, 231, and 232), confirm that same update also resolves CVE-2026-19766 rather than assuming it.
2. Segment networks to limit adjacent access to AFC hosts
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-2026-19766>