**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 231: HPE Aruba Networking Fabric Composer Stored Cross-Site Scripting Vulnerability (CVE-2026-73700).

**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, including any staff granted the lower-privileged "operator" role in the AFC web management interface. This alert is intended to be understood by technical users and systems administrators.

# What is it?

CVE-2026-73700 (CVSS 3.1 base score 9.0, Critical) is a stored cross-site scripting (XSS) vulnerability in the web-based management interface of HPE Aruba Networking Fabric Composer. An authenticated attacker holding only the low-privileged "operator" role can store malicious script content in the interface that later executes in the browser of a higher-privileged administrative user who views it, in the context of the affected interface.

CVE-2026-73700 was disclosed on 1 September 2026 in the same HPE security bulletin as CVE-2026-76657 and CVE-2026-76658, two unauthenticated authentication-bypass vulnerabilities in the same product that CERTVU addressed in Advisory 230 and Advisory 226 respectively - CVE-2026-73700 is a separate, lower-precondition flaw in the web UI rather than the same bug. Unlike those two, exploitation requires an existing low-privileged account and a victim administrator viewing the malicious content, but a successful attack executes script in that administrator's browser session,

which can be used to take actions on their behalf or otherwise compromise the administrative session within the AFC interface.

# 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)

HPE's public bulletin (docId HPESBNW05133) is the authoritative source for the specific fixed version and download package, and covers CVE-2026-73700 alongside CVE-2026-76657 and CVE-2026-76658; CERTVU could not independently verify a fixed version number at the time of writing and organizations should confirm the correct upgrade target directly against that bulletin before patching. A single upgrade is expected to address all three advisories, but administrators should confirm this against the bulletin rather than assume it.

# What does this mean?

**Typical attack flow:**

1. **Store malicious script content via a low-privileged account**
    - An attacker with an existing, low-privileged "operator" account on an affected AFC instance submits crafted input containing malicious script content that the web management interface stores without adequate sanitization.
2. **Trigger execution in an administrator's session**
    - When an administrative user later views the page containing the stored content, the malicious script executes in their browser in the context of the AFC interface, potentially allowing the attacker to act on their behalf or otherwise compromise their session.

**Attack vectors:**

- An existing, low-privileged "operator" account on the AFC web management interface — this vulnerability requires prior authentication, unlike the unauthenticated bypasses covered in Advisories 226 and 230.
- A higher-privileged administrative user subsequently viewing the attacker-controlled content within the interface.

Successful exploitation may allow attackers to:

- Execute arbitrary script code in an administrative user's browser, in the context of the AFC web management interface.
- Leverage that execution to act on the administrator's behalf or otherwise compromise their session, potentially escalating a low-privileged foothold toward administrative control of the AFC host.

# 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 or CVE-2026-76658 (Advisories 230 and 226), confirm that same update also resolves CVE-2026-73700 rather than assuming it.

2. Review and restrict operator-level account grants
3. Apply least privilege to AFC accounts 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-2026-73700