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

13 November 2026

Advisory 374: IBM Aspera Faspex Incorrect Authorization Vulnerability (CVE-2026-123218).

Release Date: 13th November 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 utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-123218 is a critical incorrect authorization vulnerability (CWE-863) in IBM Aspera Faspex 5, an enterprise platform used to send large files to and from external parties. IBM rates it CVSS 9.8. A user who can log in can craft a specific message that bypasses authorization checks and gives them full administrative privileges over the Faspex server.

What are the systems affected?

The vulnerability affects IBM Aspera Faspex 5 on Linux:

- IBM Aspera Faspex 5.0.0 through 5.0.19 (all versions before 5.0.19 PL1)
- Servers with self-registration or external user invitations enabled are at the highest risk, because any outside user can obtain the account the attack needs
- Servers still running 5.0.15.4 or earlier also carry earlier code execution flaws (CVE-2026-14958 and CVE-2026-14959) that an attacker with administrator rights could use after this bypass

Not affected / patched version:

- IBM Aspera Faspex 5.0.19 PL1, with the faspex-core container image showing 5.0.19 (1ce4b13, Fix Pack: 1)

What does this mean?

Successful exploitation may allow attackers to:

- Take full administrative control of the Faspex server
- Read, download or tamper with files exchanged with partners, clients and the public
- Create or change user accounts and settings to keep access
- Use the server as a foothold into the internal network

Mitigation process

CERTVU recommends the following:

1. Apply IBM Aspera Faspex 5.0.19 PL1
Servers on 5.0.19 can install PL1 by running faspexctl setup as root, which pulls the updated container image. Servers on 5.0.18 or earlier must first upgrade to 5.0.19 and then apply PL1. IBM lists no workaround, so applying the fix is the only complete remedy.

2. Restrict account creation until patched
Disable self-registration or switch it to administrator approval under the Account registration security setting, and review outstanding external user invitations. This reduces exposure but does not stop attacks from accounts that already exist.

Reference

1. https://www.ibm.com/support/pages/node/7295921
2. https://www.cve.org/CVERecord?id=CVE-2026-123218
3. https://nvd.nist.gov/vuln/detail/CVE-2026-123218
4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-123218
5. https://www.securityweek.com/ibm-aspera-faspex-signalwire-freeswitch-vulnerabilities-exploited-in-attacks/