contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

IBM Aspera Faspex exploited

CVE-2026-123218 · on CISA's exploited list since 9 November 2026

Analysis Report

Anyone running IBM Aspera Faspex versions 5.0.0 through 5.0.19 must upgrade to 5.0.19 PL1; the CISA deadline is 12 November 2026, two days from today. Find which version is installed and confirm Fix ...

PREPARED BY	NamiQ	DATE	11 November 2026
FACTS AS OF	11 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 12 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/ibm-aspera-faspex-cve-2026-123218

The bottom line

> *Anyone running IBM Aspera Faspex versions 5.0.0 through 5.0.19 must upgrade to 5.0.19 PL1; the CISA deadline is 12 November 2026, two days from today. Find which version is installed and confirm Fix Pack 1 is in place before anything else.*

At a glance

Fact	Detail
Product	IBM Aspera Faspex (CVE-2026-123218)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 9 November 2026. Deadline for US federal agencies: 12 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 11 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	IBM Aspera Faspex 5.0.19 PL1 (Linux). The vendor's advisory says to validate that the faspex-core container image is at 5.0.19 (image id 1ce4b13, Fix Pack: 1).
Who looks first	Any organisation running IBM Aspera Faspex on Linux, on any version from 5.0.0 through 5.0.19. If Faspex is not in your environment, nothing to do here.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run IBM Aspera Faspex anywhere on your estate?	Nothing to do for this CVE.	Check the installed version.
Is your Faspex version between 5.0.0 and 5.0.19 (inclusive)?	The record does not list other versions as affected.	Check whether Fix Pack 1 is already applied.
Has 5.0.19 PL1 (Fix Pack 1) already been applied?	Apply 5.0.19 PL1 immediately — no workaround exists.	Confirm the faspex-core image id is 1ce4b13, then no further action.

What it is

The record says an authenticated Faspex user can craft a specially formed message that causes the product to skip its authorisation check, giving that account full administrative privileges over the system.

Why it matters

The IBM CVSS score of 9.8 uses a vector that rates privileges as not required (PR:N), yet the record and the vendor's advisory both state that an authenticated user is needed. Our reading is that the discrepancy may mean any Faspex account — however low-privileged — is enough to trigger the bypass; the bar is a login, not an admin role. Because the bypass delivers full administrative access and the vendor's advisory states no workaround exists, the upgrade is the only way to close the exposure.

What the vendor's advisory says

We read one page on www.ibm.com. In short:

- The vendor's advisory, published 7 November 2026, states that 5.0.19 PL1 (Linux) addresses this flaw and that there are no workarounds or mitigations. No other CVEs are mentioned in the same release.

Things people will get wrong

- 'We're on 5.0.19 so we're already patched.' The record lists 5.0.19 as affected. The fix is specifically 5.0.19 PL1 (Fix Pack 1). The vendor's advisory says to verify that the faspex-core container image id is 1ce4b13.
- 'The CVSS vector says no privileges needed, so any outsider can exploit this.' The record and the vendor's advisory both state that an authenticated user is required. The PR:N scoring conflicts with that description; treat the record's stated condition as more specific.

The wording includes conditions the score may not show: the attacker must be logged in. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find your Faspex version and fix pack level

- Check the Faspex admin console or deployment package for the installed version and confirm whether it falls in the 5.0.0–5.0.19 range.
- The vendor's advisory says to validate the faspex-core container image id; confirm it shows 1ce4b13 (Fix Pack 1) if you are on 5.0.19.

```
docker inspect faspex-core
docker images | grep faspex
```

Step 2: Reduce exposure while preparing the upgrade

- If Faspex faces the internet and an upgrade cannot happen immediately, restrict access to trusted IP ranges at the network layer until the patch is in place.
- The vendor's advisory states no workaround exists, so this is a temporary holding measure only.

Step 3: Apply 5.0.19 PL1 (Fix Pack 1)

- Follow the upgrade instructions from the vendor's advisory (published 7 November 2026) for Linux.
- After the upgrade, the advisory says to verify the faspex-core container image id is 1ce4b13 and that Fix Pack shows as 1.

Step 4: Confirm the fix and review for signs of earlier misuse

- Re-verify the container image id, then check the administrator account list for any accounts that should not hold elevated privileges.
- Review Faspex audit logs for administrative actions performed by non-admin accounts before the patch was applied.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We run IBM Aspera Faspex and have been made aware of CVE-2026-123218, an authorisation bypass that allows any authenticated user to gain full administrative privileges. The flaw affects all versions from 5.0.0 through 5.0.19. The fixed version is 5.0.19 PL1 (Linux), which requires verifying that the faspex-core container image id is 1ce4b13 (Fix Pack 1). CISA has set a remediation deadline of 12 November 2026. Please confirm in writing: whether Faspex is installed and where, the current version and fix pack level, and whether 5.0.19 PL1 has been applied or is scheduled. We need this confirmation by 12 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- In Faspex audit logs, any administrative action — account creation, permission changes, configuration edits — carried out by a user account that does not normally hold admin rights.
- New or modified administrator accounts with creation dates falling within the period the system was exposed, particularly accounts with unfamiliar names.

The weakness behind it

The record classes this as CWE-863 (Incorrect Authorization).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	The flaw requires a valid Faspex account; any authenticated user would likely use their own credentials as the initial foothold before triggering the privilege bypass.

Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	CWE-863 describes an incorrect authorisation check; exploiting it would typically be used to escalate from a standard account to full administrative control.
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	Faspex is a file-transfer platform commonly internet-facing; a network-reachable authorisation flaw would likely be exploited via this technique if the service is exposed.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *IBM Aspera Faspex contains an incorrect authorization vulnerability that could allow an authenticated user to craft a specific message to bypass authorization, causing privilege escalations.*

The CVE record, published by Ibm on 7 November 2026:

> *IBM Aspera Faspex 5.0.0 through 5.0.19 could allow an authorized user to craft a specific message to bypass user authorization and gain full administrative privileges.*

Versions of IBM Aspera Faspex the record lists as affected:

- 5.0.0 through 5.0.19

What the record says to do about it, in the vendor's words:

> *IBM strongly recommends addressing the vulnerability now by upgrading: ProductVersionPlatformFix InstructionsIBM Aspera Faspex5.0.19 PL1Linux Please follow the instructions here https://www.ibm.com/docs/en/aspera-faspex/5.0.x . Validate that the faspex-core container image is 5.0.19 (1ce4b13, Fix Pack: 1)*

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-123218
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-123218
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- Whether the CVSS vector's PR:N rating or the advisory's 'authenticated user' language accurately describes the exploitation condition — the two conflict and the sources do not resolve this.
- The specific message format needed to trigger the authorisation bypass is not described in the record or the advisory.
- Whether versions before 5.0.0 or platforms other than Linux are affected; the record and advisory cover only 5.0.0–5.0.19 on Linux.

- We have not tested this against any environment. Versions and scores are as the sources state them and as at 11 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-123218: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
7 November 2026	CVE record published by Ibm.
9 November 2026	CISA added it to its list of exploited vulnerabilities.
12 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Faspex 5.0.0–5.0.19 reachable from the internet with multiple user accounts	High	Before 12 November 2026
Faspex 5.0.0–5.0.19 on an internal network with multiple non-admin user accounts	High	Before 12 November 2026
Faspex 5.0.0–5.0.19 accessed only by a small group of trusted administrators	Medium	This week

Faspex 5.0.19 PL1 already confirmed installed with faspex-core image id 1ce4b13	None	None for this CVE

Appendix 4. Definition of done

- Every IBM Aspera Faspex you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-123218: https://www.cve.org/CVERecord?id=CVE-2026-123218
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.ibm.com/support/pages/node/7295921: https://www.ibm.com/support/pages/node/7295921