contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

mirendev runtime: new CVE

CVE-2026-75521 · record published 18 November 2026

Analysis Report

If you run Miren Runtime below 0.11.1, upgrade to 0.11.1 and restart the server now, and check whether port 8443 is reachable from outside your management network. If you do not run Miren Runtime ...

PREPARED BY	NamiQ	DATE	19 November 2026
FACTS AS OF	19 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

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/mirendev-runtime-cve-2026-75521

The bottom line

> *If you run Miren Runtime below 0.11.1, upgrade to 0.11.1 and restart the server now, and check whether port 8443 is reachable from outside your management network. If you do not run Miren Runtime, you can stop reading.*

At a glance

Fact	Detail
Product	mirendev runtime (CVE-2026-75521)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by GitHub on 18 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 19 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	0.11.1. The vendor's advisory says to upgrade and restart the server so the new listener setting takes effect.
Who looks first	Anyone running Miren Runtime below 0.11.1 whose RPC port 8443 can be reached from networks or people you do not fully trust. Internet-facing hosts first.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Miren Runtime (the Miren application platform)?	Nothing to do for this CVE.	Check the version (next question).
Is the version below 0.11.1?	Not affected by this CVE, per the record. Confirm the restart happened after the upgrade.	Affected. Check who can reach port 8443.
Can anything outside your trusted management network reach port 8443?	Lower exposure, but still upgrade. The vendor calls network limits containment only.	Restrict access today, then upgrade and restart.

What it is

The RPC server accepts a self-signed certificate that only claims the cluster CA as its issuer, and treats its CommonName as a superuser identity. Such callers bypass all RBAC checks. Anyone who can

reach port 8443 gets full control of the cluster.

Why it matters

The record gives a score of 10 and the vendor rates it Critical. Our reading is that a forged certificate hands over the whole platform: the record lists applications, sandboxes, disks and credentials. An attacker would likely use it to read secrets, change workloads or take services down. The flaw is a certificate-validation failure (CWE-295), so no password has to be guessed.

What the vendor's advisory says

We read two pages on github.com. In short:

- The vendor's advisory says the fix verifies the client-certificate chain before trusting it, using tls.VerifyClientCertIfGiven when a cluster CA is configured.
- It says callers with no certificate, such as JWT/OIDC users who authenticate through the Authorization header, are still admitted.
- As defence in depth, both RPC authenticators now require a non-empty VerifiedChains before taking an identity from a certificate.
- Workaround until patched: remove any 0.0.0.0/0 ingress to port 8443 and limit it to trusted management networks. The advisory says this contains the risk but does not remove the flaw.
- The advisory says to restart the server after upgrading. A release alone does not change a running listener.

Things people will get wrong

- "A firewall rule fixes it." The vendor says restricting port 8443 is containment only and does not remove the flaw. Upgrade to 0.11.1 and restart.
- "The attacker needs a valid certificate from our CA." No. The record says a self-signed certificate with an issuer name matching the public cluster CA subject is enough.
- "We upgraded, so we are safe." The vendor says to restart the server so the new listener configuration takes effect.

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 the versions you run

- List every host running Miren Runtime and note its version. The record says anything below 0.11.1 is affected.
- Check whether the server was restarted after any upgrade.

```
miren version
ss -lun | grep 8443
```

Step 2: Reduce exposure to port 8443

- Remove any ingress open to all addresses and allow only trusted management networks, as the vendor suggests.
- Treat this as a stopgap, since the advisory says it does not remove the flaw.

Step 3: Upgrade and restart

- Upgrade to 0.11.1 and restart the server so the new listener setting is used.

Step 4: Check for signs of misuse

- If port 8443 was reachable by untrusted networks, review who connected and what changed in applications, disks and credentials. Rotate credentials if anything looks wrong.

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.

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.

> *Hello, we need to know whether we run Miren Runtime (mirendev) and, if so, where and which version. CVE-2026-75521 affects versions below 0.11.1 and lets a network attacker with a forged certificate gain cluster superuser access through port 8443. Please tell us whether port 8443 is reachable from untrusted networks. Please upgrade to 0.11.1, restart the server, and confirm in writing the version and that the restart is done, by an agreed date. Thank you.*

The weakness behind it

The record classes this as CWE-295.

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
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	The listener on port 8443 is reachable over a network and accepts a forged certificate, so a remote attacker would likely use it as the way in.
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 forged certificate is taken as a valid superuser identity, so the attacker would typically act as a legitimate administrator.

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

The CVE record:

> *Miren Runtime provides the runtime component for the Miren application platform. Prior to 0.11.1, the QUIC/HTTP3 RPC server on the default port 8443 uses tls.RequestClientCert and does not verify that presented certificates chain to the configured cluster certificate authority. The RPC authenticators derive a caller identity from PeerCertificates[0].Subject.CommonName without requiring a non-empty VerifiedChains value, and certificate identities bypass all RBAC checks. A network attacker who can reach the listener can present a self-signed certificate with an issuer distinguished name matching the public cluster CA subject and gain cluster superuser access, allowing disclosure …*

Versions of mirendev runtime the record lists as affected:

- < 0.11.1

The record gives no version ranges. Use the vendor's advisory for the affected versions.

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-2026-75521
```

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-2026-75521
```

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

- No source says whether this flaw is being exploited. It was a new record and not on CISA's list when read.
- The sources do not say how many releases before 0.11.1 are affected, only that all below it are.
- The record does not say how to tell from logs that a forged certificate was used.
- The sources do not say whether other Miren components are affected.
- Exploitation is not recorded. That is not the same as none.

- This is a new record: scores, versions and wording can change in the first days, and they are as at 19 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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-2026-75521: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H` As the CVE record gives it.

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.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
18 November 2026	CVE record published by GitHub.

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
Miren Runtime below 0.11.1 with port 8443 open to the internet	Medium	Today: restrict access, then upgrade

Miren Runtime below 0.11.1, port 8443 reachable from a wider internal network	Medium	This week, after restricting access
Miren Runtime below 0.11.1, port 8443 limited to a small trusted management network	Medium	Next planned change window, soon
Miren Runtime 0.11.1 upgraded but the server not restarted	Medium	Restart now
You do not run Miren Runtime	None	None for this CVE

Appendix 4. Definition of done

- Every mirendev runtime you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-75521: https://www.cve.org/CVERecord?id=CVE-2026-75521
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/mirendev/runtime/security/advisories/GHSA-8fh7-: https://github.com/mirendev/runtime/security/advisories/GHSA-8fh7-7q4q-cq52
- Advisory or release notes read: github.com/mirendev/runtime/releases/tag/v0.11.1: https://github.com/mirendev/runtime/releases/tag/v0.11.1
- Reference in the CVE record: github.com: https://github.com/mirendev/runtime/commit/e2159c8c8559da3f1c1485b463c794d656cd2fe4