contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

19 November 2026 · 3 new critical CVEs worth reading

Analysis Report

260 new records scored 8 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	19 November 2026
FACTS AS OF	19 November 2026	VERSION	1.0
TOP SCORE	Critical: 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/daily-cve-highlight-2026-11-19

The bottom line

> *All three score 10. Incus and Miren Runtime accept certificates they did not properly check; cf-manager is a different flaw. One question sorts them: do you run any of these, and can anyone you do not trust reach it?*

880 CVE records were published in the last 30 hours. 260 scored 8 or higher. 3 are below, chosen by a fixed rule: highest score first, then fewest conditions in the wording, one product each. None is on CISA's exploited list, so a score here is the record's author describing the worst case. Read the condition before you act on the number.

At a glance

Product	Score	Fixed in	Read next
lxc incus (CVE-2026-130778)	10 (CVSS 4.0)	Incus 7.6.0 (the vendor's advisory, 29 October 2026; the record lists 7.6.0 as unaffected).	Technical Analysis
hefy2027 cf-manager (CVE-2026-71499)	10 (CVSS 3.1)	cf-manager 1.1.2. Both the CVE record and the project's release notes name it as the fixed version.	Technical Analysis
mirendev runtime (CVE-2026-75521)	10 (CVSS 4.0)	0.11.1. The vendor's advisory says to upgrade and restart the server so the new listener setting takes effect.	Technical Analysis

lxc incus, CVE-2026-130778

Run Incus before 7.6.0 with a reachable HTTPS listener? Restrict access to trusted hosts now, then upgrade to 7.6.0 (vendor advisory, 29 October 2026). Not running it: nothing to do.

Score 10 (CVSS 4.0), published by VulnCheck on 18 November 2026. Weakness: CWE-287.

A remote client can act as any trusted certificate by appending its public part to its own TLS chain, with no private key. That gives cluster-level access. Affects Incus before 7.6.0. The record states no limiting condition.

hefy2027 cf-manager, CVE-2026-71499

If you run cf-manager, check API_SECRET is set, then upgrade to 1.1.2 this week. Both the record and the release notes name 1.1.2 as fixed. Otherwise nothing to do.

Score 10 (CVSS 3.1), published by GitHub on 18 November 2026. Weakness: CWE-94, CWE-918.

It fetches any URL it is given and deploys the result as a Worker script with stored Cloudflare credentials. Affects cf-manager before 1.1.2. Limit: the attacker needs deployment API access, unless

API_SECRET is not set.

mirendev runtime, CVE-2026-75521

Upgrade Miren Runtime to 0.11.1 and restart the server now, as the vendor's advisory says. Check whether port 8443 is reachable beyond your management network. Otherwise nothing to do.

Score 10 (CVSS 4.0), published by GitHub on 18 November 2026. Weakness: CWE-295.

A forged self-signed certificate naming the cluster CA as issuer gets superuser access, skipping RBAC, on the RPC port 8443. Affects Miren Runtime before 0.11.1. Limit: the attacker must be able to reach that listener.

Fifteen minutes this morning

- List the products above you run. If none, you are done.
- For each one you run, read the version from the product and compare it to the fixed version in the table.
- If it is in range, follow the note: reduce exposure first, then update.
- Book the update, and write down who owns it and by when.

Check your own project

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

```
lattice-scan project . --cve CVE-2026-130778,CVE-2026-71499,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 ids 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-2026-130778 --cve CVE-2026-71499 --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

- These are new records. A record can change in the first days: scores, versions and wording are as at 19 November 2026. Nothing here has been tested.
- Exploitation is not recorded for any of them. That is not the same as none.
- The bottom line and the sentence under each product are our interpretation of the records and the vendors' pages, not a statement by the vendors.

Appendix 1. Severity decoded

CVE-2026-130778: 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`

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.

CVE-2026-71499: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`

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	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

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`

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	lxc incus, CVE-2026-130778: record published by VulnCheck.
18 November 2026	hefy2027 cf-manager, CVE-2026-71499: record published by GitHub.
18 November 2026	mirendev runtime, CVE-2026-75521: record published by GitHub.

Appendix 3. Definition of done

- The products above you run are listed, with versions.
- Each in range has the vendor's fixed version and mitigation noted.
- The update is booked, with an owner and a date.
- Anything not in range is recorded as checked.

Sources

- CVE record service: https://www.cve.org/
- CVE record for CVE-2026-130778: https://www.cve.org/CVERecord?id=CVE-2026-130778
- CVE record for CVE-2026-71499: https://www.cve.org/CVERecord?id=CVE-2026-71499
- CVE record for CVE-2026-75521: https://www.cve.org/CVERecord?id=CVE-2026-75521