contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Cribl Stream: new CVE

CVE-2026-115873 · record published 23 November 2026

Analysis Report

CVE-2026-115873 in Cribl Stream, a new record scored 9.9 and not on CISA's exploited list when we read it. What it is, who is affected, and what to check first.

PREPARED BY	NamiQ	DATE	23 November 2026
FACTS AS OF	23 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	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/cribl-stream-cve-2026-115873

The bottom line

> *Check whether you run Cribl Stream. If you do, read the vendor's page for the fixed version and update. Nothing public says yet that anyone is using this flaw.*

At a glance

Fact	Detail
Product	Cribl Stream (CVE-2026-115873)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by Cribl on 23 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 23 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	The record carries the vendor's remediation text; it is quoted below

A word search of the record found none of the usual conditions (privileges, a logged-in user, a non-default setting, local network, physical access, a click). That is a search, not a reading, so read the record yourself before you rule it out.

What to do first

- Check the version you run against the versions listed under the sources, then read the vendor's page for the fixed version and any mitigation.

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.

The weakness behind it

The record classes this as CWE-94.

The sources, in their words

The CVE record:

> *A remote attacker must authenticate with Read Only (GroupRead) access to at least one Worker Group and reach the Leader API. A crafted expression can exploit the nested compiler to bypass expression restrictions and execute code with the Leader service account's permissions.*

Versions of Cribl Stream the record lists as affected:

- all versions up to and including 4.20.4

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

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

> *Upgrade Cribl Stream to v4.21.*

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-2026-115873
```

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-2026-115873
```

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

- 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 23 November 2026. We have not read the vendor's advisory page and we have not tested it.

Appendix 1. Severity decoded

CVE-2026-115873: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A: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.
Privileges required	Low	An ordinary account is enough.
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.

Appendix 2. Timeline

Date	Event
23 November 2026	CVE record published by Cribl.

Appendix 3. Definition of done

- Every Cribl Stream 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-2026-115873: https://www.cve.org/CVERecord?id=CVE-2026-115873
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: trust.cribl.io: https://trust.cribl.io/notifications
- Reference in the CVE record: csaf.cribl.io: https://csaf.cribl.io/2026/cribl-2026-0006.json