contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

16 November 2026 · 3 new critical CVEs worth reading

Analysis Report

66 new records scored 8.5 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	16 November 2026
FACTS AS OF	16 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-2026-11-16

The bottom line

> *These three records are unrelated: different products, different weaknesses. One question sorts them. Do you run Phoenix, the Station Launcher App in 3DEXPERIENCE, or Tensei with @tensei/auth? If not, you can stop reading.*

389 CVE records were published in the last 30 hours. 66 scored 8.5 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
Arize-ai phoenix (CVE-2026-53998)	10 (CVSS 3.1)	15.7.0. The record says it is fixed there. The release notes dated 13 May 2026 list 'prevent format-string injection in f-string template formatter'.	Technical Analysis
Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform (CVE-2026-93664)	10 (CVSS 3.1)	See the note	Technical Analysis
tenseijs @tensei/auth (CVE-2026-129552)	9.8 (CVSS 3.1)	See the note	Technical Analysis

Arize-ai phoenix, CVE-2026-53998

If you run Phoenix from 13.0.0 up to before 15.7.0, update to 15.7.0 this week; the record says it is fixed there. First check whether untrusted people can reach the service.

Score 10 (CVSS 3.1), published by GitHub on 16 November 2026. Weakness: CWE-134, CWE-200.

A crafted template sent to the applyChatTemplate query lets an attacker read server environment variables, including PHOENIX_SECRET, which the record says can lead to forged admin tokens. With authentication on, any account can reach it.

Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform, CVE-2026-93664

If you use the Station Launcher App, ask Dassault Systèmes or your IT provider this week which release you run. The sources we read do not name a fixed release.

Score 10 (CVSS 3.1), published by 3DS on 16 November 2026. Weakness: CWE-502.

The record says untrusted serialised data in the Station Launcher App could let an attacker run their own code with no login. It gives no detail on how the attack is delivered. The record states no limiting condition.

tenseijs @tensei/auth, CVE-2026-129552

If you run Tensei with @tensei/auth, check today that JWT_SECRET is set, and set it if not. No fixed version is named, so do not wait for one. Treat past administrator activity as suspect.

Score 9.8 (CVSS 3.1), published by VulnCheck on 16 November 2026. Weakness: CWE-1394.

When JWT_SECRET is unset, @tensei/auth signs tokens with a key written in its code, so anyone can forge a token for any user, including an administrator. It only applies when JWT_SECRET is unset.

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-2026-53998,CVE-2026-93664,CVE-2026-129552
```

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-2026-53998 --cve CVE-2026-93664 --cve CVE-2026-129552
```

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 16 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-2026-53998: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L`

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	Low	Reduced performance or interruptions.

CVE-2026-93664: 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-2026-129552: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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	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
16 November 2026	Arize-ai phoenix, CVE-2026-53998: record published by GitHub.
16 November 2026	Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform, CVE-2026-93664: record published by 3DS.
16 November 2026	tenseijs @tensei/auth, CVE-2026-129552: record published by VulnCheck.

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-2026-53998: https://www.cve.org/CVERecord?id=CVE-2026-53998
- CVE record for CVE-2026-93664: https://www.cve.org/CVERecord?id=CVE-2026-93664
- CVE record for CVE-2026-129552: https://www.cve.org/CVERecord?id=CVE-2026-129552