contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform: new CVE

CVE-2026-93664 · record published 16 November 2026

Analysis Report

PREPARED BY	NamiQ	DATE	16 November 2026
FACTS AS OF	16 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 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/dassault-syste-mes-station-launcher-app-in-cve-2026-93664

The bottom line

> *If you run the 3DEXPERIENCE platform with the Station Launcher App, ask your IT provider or Dassault Systèmes this week which release you are on and whether a fix exists. If you do not use 3DEXPERIENCE, you can stop reading.*

At a glance

Fact	Detail
Product	Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform (CVE-2026-93664)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by 3DS on 16 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 16 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Organisations running Dassault Systèmes 3DEXPERIENCE, releases R2023x to R2026x, with the Station Launcher App. Whoever administers that platform should check first.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run the Dassault Systèmes 3DEXPERIENCE platform?	Nothing to do for this CVE.	Check whether the Station Launcher App is in use.
Is the Station Launcher App installed or used in your 3DEXPERIENCE setup?	The record lists only this app, so there is nothing further for this CVE.	Find your release (next question).
Is your release between R2023x and R2026x, up to the listed fix-pack levels?	Ask the vendor to confirm in writing that your release is not affected.	Treat the system as exposed and contact the vendor now.
Can untrusted networks or users reach the Station Launcher App?	Lower urgency, but still plan the fix.	Reduce that exposure first, then patch.

What it is

The record says the Station Launcher App can be made to process untrusted serialised data. That could let someone with no login run their own code on the system. The record gives no further detail on how the attack is delivered.

Why it matters

Our reading is that unauthenticated code execution on a platform that holds design and engineering data is worth an early look, even though CISA does not list this CVE as exploited. The record gives it a score of 10 and the vendor calls it critical. The weakness is untrusted deserialisation, CWE-502.

What the vendor's advisory says

We read one page on www.3ds.com. In short:

- The vendor's advisory page repeats the record: untrusted deserialisation in the Station Launcher App could lead to unauthenticated remote code execution.
- It lists the affected versions as R2023x through R2026x and rates the severity critical.
- It points to remediation information on the vendor's security advisories page. The text we hold does not name a fixed release or a workaround.

Things people will get wrong

- "It is not on the CISA list, so it is not urgent." The record is new. The record says no login is needed, and it scores 10. Absence from the CISA list means little this early.
- "We are on a recent release, so we are fine." The record lists releases from R2023x through R2026x, each up to a named fix-pack level. Recent releases are inside that range.
- "A fixed version is out, so we just update." The sources we hold do not name a fixed version. Ask the vendor what remediation exists for your release.

How we would triage it

This is our judgement.

Step 1: Find out whether you run it

- Ask whoever administers 3DEXPERIENCE whether the Station Launcher App is installed and who uses it.
- Note the release and fix-pack level, and compare them with the affected ranges on this page.

Step 2: Reduce exposure

- Find out whether the app can be reached from the internet or from untrusted networks.
- If it can, ask your provider to restrict access until a fix is confirmed.

Step 3: Get the remediation from the vendor

- Read the vendor's security advisory and remediation page for your release. The record names no fixed version.
- Apply what the vendor specifies and keep a written record of the version before and after.

Step 4: Check for signs of misuse

- Ask your provider to review logs for the app and its host for unexpected requests or new processes.
- Treat any unexplained activity as a possible compromise.

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 have seen CVE-2026-93664, a deserialisation flaw in the Station Launcher App in the Dassault Systèmes 3DEXPERIENCE platform. The record says it could allow unauthenticated remote code execution. Please tell us whether we run 3DEXPERIENCE and the Station Launcher App, where, and which release and fix-pack level. Please also tell us whether it can be reached from outside our network. The sources we have do not name a fixed version, so please ask the vendor for its remediation. Please confirm the version and the fix to us in writing by the end of this week.*

The weakness behind it

The record classes this as CWE-502.

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 record says unauthenticated remote code execution. That would likely let an attacker gain initial access by sending crafted data to an exposed service.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	Code execution from untrusted deserialised data would typically be used to run commands or scripts on the host.

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:

> *A Deserialization of Untrusted Data vulnerability affecting Station Launcher App in 3DEXPERIENCE platform from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2026x could lead to an unauthenticated remote code execution.*

Versions of Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform the record lists as affected:

- Release 3DEXPERIENCE R2023x Golden through Release 3DEXPERIENCE R2023x.FP.CFA.2613
- Release 3DEXPERIENCE R2024x Golden through Release 3DEXPERIENCE R2024x.FP.CFA.2632
- Release 3DEXPERIENCE R2025x Golden through Release 3DEXPERIENCE R2025x.FP.CFA.2637
- Release 3DEXPERIENCE R2026x Golden through Release 3DEXPERIENCE R2026x.FP.CFA.2635

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-2026-93664
```

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-2026-93664
```

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

- Which release or fix pack fixes this flaw. The sources we hold name none.
- Whether a workaround exists short of patching.
- How the attack reaches the app, and whether the app listens on a network port by default.
- Whether anyone is exploiting it. It is a new record.
- 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 16 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-2026-93664: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/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	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.

Appendix 2. Timeline

Date	Event
16 November 2026	CVE record published by 3DS.

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
Station Launcher App on an affected release, reachable from the internet	High	now; contact the vendor today
Affected release, reachable only from your internal network	Medium	this week
Affected release, but the app is not installed or not in use	Low	confirm in writing, then next patch cycle
No 3DEXPERIENCE platform in your estate	None	none for this CVE

Appendix 4. Definition of done

- Every Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform 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-2026-93664: https://www.cve.org/CVERecord?id=CVE-2026-93664
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.3ds.com/trust-center/security/security-advisories/cve-2: https://www.3ds.com/trust-center/security/security-advisories/cve-2026-93664