contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

tenseijs @tensei/auth: new CVE

CVE-2026-129552 · record published 16 November 2026

Analysis Report

If you run a Tensei site that uses the auth package, check now whether its JWT secret is set. If it is not, set one and treat any past administrator activity as suspect. No fixed version is named, so …

PREPARED BY	NamiQ	DATE	16 November 2026
FACTS AS OF	16 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	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/tenseijs-tensei-auth-cve-2026-129552

The bottom line

> *If you run a Tensei site that uses the auth package, check now whether its JWT secret is set. If it is not, set one and treat any past administrator activity as suspect. No fixed version is named, so do not wait for one. Everyone else can stop reading.*

At a glance

Fact	Detail
Product	tenseijs @tensei/auth (CVE-2026-129552)
Severity	Critical: 9.8 (CVSS 3.1)
Status	A new CVE record, published by VulnCheck 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	Anyone running Tensei with the auth package, version 0.11.5 or earlier, where the JWT secret setting was never given a value. Developers, agencies and the IT provider who built or hosts the site.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a website or API built on Tensei, the Node.js content system?	Nothing to do for this CVE.	Check whether it uses the auth package (next question).
Is the auth package installed at version 0.11.5 or earlier?	Nothing to do for this CVE, as far as the record shows.	Check whether the JWT secret is set (next question).
Is the JWT secret setting empty or missing in the live environment?	The fixed-key fallback is not used. Still confirm the secret is long and random.	Treat the site as open to forged logins. Set a secret and review activity.
Can anyone on the internet reach the site's login or API?	Lower urgency, but fix it at the next change window.	Act today: no login is needed to exploit it.

What it is

Without a JWT secret set, the auth package signs login tokens with a fixed key written into its code. Anyone who knows that key can make a token for any user id, including an administrator, and the site accepts it with no login.

Why it matters

Our reading is that this flaw is dangerous because the key is public in the project's code and the attacker needs no account. A forged administrator token would let them read or change anything the site holds. The same public issue lists other flaws in the same release, so setting a secret may not make the site safe by itself.

What the vendor's advisory says

We read three pages on www.vulncheck.com and github.com. In short:

- The public issue, opened on 15 November 2026 by a researcher, reports several flaws in Tensei 0.11.5, not only this one.
- It lists unauthenticated file upload, with a client-chosen storage path that allows writing outside the storage folder.
- It lists fail-open authorization: a resource with no access rule is open to anonymous users, and users may be able to give themselves privileged roles.
- The issue also names filtering, CSRF and social sign-in problems in its title. The excerpt does not describe them.
- The excerpt shows no reply from the maintainers and no fixed release. The issue was still open when read.

Things people will get wrong

- "It is not on the CISA list, so it can wait." A new record is not yet listed by CISA. It needs no login over a network, and the issue is public, so waiting gains nothing.
- "Setting the secret makes the site safe." The public issue reports other flaws in the same release, such as open file upload and missing access rules. This CVE covers only the signing key.

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 where Tensei runs and which version

- Ask your developer or host which sites use Tensei. The record covers the auth package, version 0.11.5 and earlier.
- Check each project's installed package versions.

```
npm ls @tensei/auth
npm ls --all
```

Step 2: Check whether the JWT secret is set

- Confirm the live environment gives the JWT secret a long random value. If it is empty, the fixed key is in use.
- Do not copy the value into tickets or emails.

Step 3: Set a secret and limit exposure

- Set a long random JWT secret and restart the service. Tokens signed with the old key should then stop working.
- Where possible, limit who can reach the login and API until the other reported flaws are reviewed.

Step 4: Review what happened

- Look for administrator activity you cannot account for, and for new or changed users and roles.
- Ask the maintainers or your developer whether a fixed release exists. The sources name none.

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-2026-129552 in the Tensei content system. Its auth package, version 0.11.5 and earlier, uses a fixed signing key when no JWT secret is set. That lets an outsider impersonate any user, including an administrator. Please tell us whether we run Tensei, where, and which auth package version. Please also confirm whether the JWT secret is set. The sources name no fixed version. Please confirm in writing by the end of this week the version, the secret setting and any other steps taken.*

The weakness behind it

The record classes this as CWE-1394.

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 flaw is reachable over a network with no login, so it would likely be used against an internet-facing Tensei site.
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	A forged token lets an attacker act as a real user or administrator, so it would typically be used like a stolen valid account.

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:

> *Tensei through 0.11.5 contains an authentication bypass vulnerability in @tensei/auth that falls back to the hard-coded JWT signing key 'auth-secret-key' when JWT_SECRET is unset. Unauthenticated attackers can sign tokens with arbitrary user ids accepted by populateContextFromToken to impersonate any user, including administrators.*

Versions of tenseijs @tensei/auth the record lists as affected:

- all versions up to and including 0.11.5

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-2026-129552
```

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 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-2026-129552
```

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

- Whether the maintainers have released a fixed version. The sources name none.
- Whether any attacker has used this flaw. The record gives no sign of it.
- Whether other Tensei packages are affected by this CVE. The record lists only the auth package.
- Whether the other flaws in the public issue have CVE ids or fixes. The excerpt does not say.
- 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-2026-129552: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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	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	CVE record published by VulnCheck.

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
Public Tensei site on 0.11.5 or earlier with the JWT secret unset	High	Today; no login is needed
Tensei site on an affected version, secret set to a long random value	Medium	This week: confirm the value and review the other reported flaws
Tensei site only reachable on an internal network, secret unset	Medium	This week
Tensei site where the auth package is not installed	Low	Next patch cycle; the record covers only the auth package

No Tensei anywhere in your estate	None	None for this CVE

Appendix 4. Definition of done

- Every tenseijs @tensei/auth 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-2026-129552: https://www.cve.org/CVERecord?id=CVE-2026-129552
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.vulncheck.com/advisories/tensei-through-0.11.5-authentication: https://www.vulncheck.com/advisories/tensei-through-0.11.5-authentication-bypass-via-hard-coded-jwt-secret-in-tensei-auth
- Advisory or release notes read: github.com/tenseijs/tensei/issues/398: https://github.com/tenseijs/tensei/issues/398
- Advisory or release notes read: github.com/tenseijs/tensei: https://github.com/tenseijs/tensei
- Reference in the CVE record: github.com: https://github.com/tenseijs/tensei/blob/630f39038c7751178465f990fb358b0c2d5b1914/packages/auth/src/index.ts#L94-L98