contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

surrealdb: new CVE

CVE-2026-134292 · record published 21 November 2026

Analysis Report

Anyone running SurrealDB between version 1.0.0 and 3.x with restricted user accounts should update to 4.0.0; there is no CISA deadline but the score is 9.8. If only fully trusted administrators ...

PREPARED BY	NamiQ	DATE	22 November 2026
FACTS AS OF	22 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/surrealdb-cve-2026-134292

The bottom line

> *Anyone running SurrealDB between version 1.0.0 and 3.x with restricted user accounts should update to 4.0.0; there is no CISA deadline but the score is 9.8. If only fully trusted administrators connect to your SurrealDB instance, risk is lower — confirm the version first.*

At a glance

Fact	Detail
Product	surrealdb (CVE-2026-134292)
Severity	Critical: 9.8 (CVSS 3.1)
Status	A new CVE record, published by VulnCheck on 21 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 22 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	SurrealDB 4.0.0, per the GitHub security advisory GHSA-5w6j-qm42-4rc2 published 3 November 2026 and the VulnCheck record published 21 November 2026.
Who looks first	Teams running SurrealDB 1.0.0 up to 3.x where more than one person or service account connects and not all of them hold full administrative rights.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run SurrealDB anywhere in your infrastructure?	Nothing to do for this CVE.	Check which version is installed.
Is the installed version 1.0.0 up to but not including 4.0.0?	Not affected; no action needed.	Continue to the next question.
Do any users connect with restricted permissions rather than full administrative rights?	Risk is lower; update at the next maintenance window.	Update to 4.0.0 promptly.

What it is

An authenticated database user blocked from certain built-in functions in SurrealQL can call those same functions through the embedded JavaScript scripting engine, bypassing the access controls the database applies to that user's account.

Why it matters

The record carries a CVSS 3.1 score of 9.8; VulnCheck also reports a CVSS 4.0 score of 9.3 — both in the critical band. The VulnCheck CVSS 4.0 vector marks no privileges required (PR:N), but the record's written description specifies authenticated users. Our reading is that the description is the more precise statement and that an existing database account is needed. That narrows the risk for single-operator deployments but leaves multi-user environments exposed: any restricted user can call built-in functions that their capability profile is meant to block. The practical question is whether untrusted people hold database accounts.

What the vendor's advisory says

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

- The GitHub advisory GHSA-5w6j-qm42-4rc2, published 3 November 2026, covers only this flaw. It names 4.0.0 as the patched version and states the fix enforces capability checks inside the JavaScript built-in bridge before delegating to internal dispatchers.
- The GitHub advisory lists no CWE identifiers. The VulnCheck record published 21 November 2026 assigns CWE-862 (Missing Authorization) and states the affected range as version 1.0.0 up to but not including 4.0.0.

Things people will get wrong

- The CVSS vector says no login is needed, so anyone on the network can exploit this. The VulnCheck CVSS 4.0 vector marks PR:N, but the record's written description specifies authenticated users. The discrepancy is unresolved in the sources; treat authentication as required until a source confirms otherwise.
- Blocking the database port from the internet is a sufficient fix. Network restriction reduces exposure but does not remove it. Any authenticated user already able to reach the database can bypass function controls in an unpatched version.

The wording includes conditions the score may not show: authenticated. Read the record before you decide it does not apply to you.

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 the SurrealDB version you run

- Ask your database administrator which version of SurrealDB is installed on each system; versions 1.0.0 up to but not including 4.0.0 are affected per the record.
- If SurrealDB is running as a service, the version appears in its startup log or can be printed with the CLI.

```
surreal version
```

Step 2: Identify who connects and with what permissions

- List every account with access to your SurrealDB instance and note which hold restricted rather than full administrative permissions.
- Accounts with restricted permissions are the ones the bypass is available to in an unpatched version.

Step 3: Update to SurrealDB 4.0.0 and confirm

- The vendor's advisory names 4.0.0 as the patched release. Install it, restart the service, and check the version to confirm the update applied.
- If a staged rollout is needed, prioritise instances reachable by restricted user accounts first.

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.

> *We are reviewing CVE-2026-134292, a capability check bypass in SurrealDB versions 1.0.0 up to but not including 4.0.0. The flaw allows an authenticated database user denied access to certain built-in functions to call those functions through the embedded JavaScript engine. The fixed version is 4.0.0 per the vendor's advisory. Could you please confirm: whether we run SurrealDB anywhere and on which systems; which version is installed; whether any accounts with restricted permissions connect to it; and whether we are already on 4.0.0 or can update to it. We would appreciate written confirmation of the installed version and fix status by 29 November 2026.*

The weakness behind it

The record classes this as CWE-862.

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
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	An authenticated user with restricted permissions exploits the missing capability check to access functions beyond their profile, which would typically escalate their effective access within the database.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The bypass is exercised through the embedded JavaScript scripting engine; script execution is the mechanism by which restricted built-in functions are reached.
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	If the CVSS PR:N vector is correct and no authentication is needed, a network-reachable SurrealDB instance would likely be reachable as a public-facing application for initial access.

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:

> *SurrealDB 1.0.0 before 4.0.0 contains a capability check bypass in its embedded JavaScript scripting engine, where the surrealdb.functions bridge calls the internal fnc::synchronous() and fnc::asynchronous() dispatchers without enforcing function capability checks. Authenticated users denied access to built-in functions in SurrealQL can execute them by calling them through surrealdb.functions from embedded JavaScript.*

Versions of surrealdb the record lists as affected:

- 1.0.0 up to, but not including, 4.0.0

It lists these as unaffected:

- 4.0.0

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-2026-134292
```

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-2026-134292
```

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 authentication is truly required: the CVSS 4.0 vector marks PR:N but the record description says authenticated users; the sources do not resolve this discrepancy.
- Which specific built-in functions can be reached through the JavaScript bypass and what access they grant to a restricted user.
- Whether the embedded JavaScript scripting engine can be disabled as a temporary workaround; the sources do not describe an interim mitigation short of upgrading.
- Whether versions before 1.0.0 are affected; the VulnCheck record's lower bound is 1.0.0 and earlier releases are not addressed.
- 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 22 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-2026-134292: 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
21 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
SurrealDB 1.0.0–3.x with multiple users at different permission levels	Medium	This week
SurrealDB 1.0.0–3.x accessed only by a single fully trusted administrator	Medium	Next patch cycle
SurrealDB 4.0.0 or later installed	None	None for this CVE
SurrealDB not deployed in this environment	None	None for this CVE

Appendix 4. Definition of done

- Every surrealdb 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-2026-134292: https://www.cve.org/CVERecord?id=CVE-2026-134292
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/surrealdb/surrealdb/security/advisories/GHSA-5w: https://github.com/surrealdb/surrealdb/security/advisories/GHSA-5w6j-qm42-4rc2
- Advisory or release notes read: www.vulncheck.com/advisories/surrealdb-1.0.0-before-4.0.0-functio: https://www.vulncheck.com/advisories/surrealdb-1.0.0-before-4.0.0-function-capability-bypass-via-javascript-built-in-bridge