contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

budibase server: new CVE

CVE-2026-137498 · record published 26 November 2026

Analysis Report

Anyone running Budibase server between 3.39.18 and 3.x must upgrade to 4.0.0 without delay; the flaw requires no login. Check first whether any published app exposes a MongoDB query with PUBLIC ...

PREPARED BY	NamiQ	DATE	27 November 2026
FACTS AS OF	27 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/budibase-server-cve-2026-137498

The bottom line

> *Anyone running Budibase server between 3.39.18 and 3.x must upgrade to 4.0.0 without delay; the flaw requires no login. Check first whether any published app exposes a MongoDB query with PUBLIC execution permission, as that is the specific condition the advisory describes.*

At a glance

Fact	Detail
Product	budibase server (CVE-2026-137498)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by VulnCheck on 26 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 27 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	@budibase/server 4.0.0, as named in the vendor's advisory (GHSA-x4w8-596q-fmh7) and the VulnCheck record.
Who looks first	Teams running Budibase server 3.39.18 up to but not including 4.0.0, where a published app connects to a MongoDB datasource and exposes at least one query with PUBLIC execution permission.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Budibase server anywhere on your estate?	Nothing to do for this CVE.	Check which version is installed.
Is the installed version 3.39.18 or later but earlier than 4.0.0?	Not in the affected range; no action needed.	Check whether any published app uses a MongoDB datasource with PUBLIC queries.
Does any published app connect to a MongoDB datasource with a query set to PUBLIC execution permission?	No PUBLIC MongoDB queries; upgrade at next cycle as good practice.	Upgrade to 4.0.0 immediately.

What it is

An unauthenticated attacker can send a single request to a Budibase query endpoint and erase the MongoDB filter, leaving it empty. That empty filter causes the database to return every document in the collection, or to modify or delete every document, depending on which query type is exposed.

Why it matters

The advisory says the app ID and query ID needed to reach the endpoint appear in a published app's normal requests, so an attacker with any access to the app can discover them. No session, no CSRF token, and no Budibase account is required. A single crafted request can empty an entire MongoDB collection, overwrite every record, or delete everything the query covers. Our reading is that the preconditions are genuinely low for any organisation whose Budibase apps are reachable by untrusted users, which makes the near-maximum score credible even without confirmed exploitation.

What the vendor's advisory says

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

- The vendor's advisory (GHSA-x4w8-596q-fmh7) names 4.0.0 as the patched version and states the flaw was introduced as a regression when fixing CVE-2026-54350.
- The advisory does not describe a workaround short of upgrading, and names no other CVEs as fixed in the same release.

Things people will get wrong

- Only authenticated users can reach the query endpoint The advisory states PUBLIC queries bypass both authentication and CSRF checks entirely; no session or account is required to call the endpoint.
- Only read queries are at risk; our data cannot be changed or deleted The advisory explicitly confirms that PUBLIC updateMany or deleteMany queries allow modification or deletion of every document in the collection.
- ReCAPTCHA protects our PUBLIC MongoDB queries from this attack The advisory states the attack applies when reCAPTCHA is disabled or when the caller can satisfy it; reCAPTCHA alone is not a reliable barrier.

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 Budibase server version you run

- Check your installed @budibase/server package version; the affected range is 3.39.18 up to but not including 4.0.0.

```
npm list @budibase/server
```

Step 2: Identify any PUBLIC MongoDB queries in published apps

- In the Budibase builder, review every app's data sources for MongoDB connections.
- For each MongoDB datasource, check whether any query has its execution permission set to PUBLIC and uses a request parameter as a JSON key.

Step 3: Upgrade to @budibase/server 4.0.0

- The vendor's advisory names 4.0.0 as the patched version; follow your normal Budibase upgrade procedure.
- Confirm the version is active after restart before re-enabling external access.

Step 4: Review MongoDB collections for unexpected changes

- If any PUBLIC MongoDB query was accessible before the upgrade, check whether query results returned more records than expected or whether data has changed without a known cause.

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 writing about CVE-2026-137498, a critical vulnerability in Budibase server. Versions from 3.39.18 up to but not including 4.0.0 are affected. An unauthenticated attacker can erase MongoDB query filters and read, modify, or delete every document in a collection with a single request. The patched version is 4.0.0. Could you please confirm: whether we run Budibase server; which version is installed; and whether any published app exposes a MongoDB query with PUBLIC execution permission? Please confirm in writing that version 4.0.0 is in place, or provide a date by which the upgrade will be complete.*

The weakness behind it

The record classes this as CWE-943.

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 authentication against a web query endpoint; exploiting a public-facing application would likely be the initial access technique.
Data Manipulation: Stored Data Manipulation (T1565.001): Changing stored data without permission.	Impact: causing damage or disruption	The erased filter enables updateMany against every document in the collection; this would typically be used for stored data manipulation once the endpoint is reached.
Data Destruction (T1485): Deleting or overwriting data so it cannot be recovered.	Impact: causing damage or disruption	The empty filter enables deleteMany against an entire collection; the advisory confirms full-collection deletion as a confirmed availability impact of the flaw.

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:

> *Budibase Server from 3.39.18 before 4.0.0 contains a prototype pollution vulnerability that allows unauthenticated attackers to erase MongoDB query filters by supplying __proto__ as a dynamic JSON key in PUBLIC queries. Attackers can send a single request to the query execution endpoint, reducing the filter to {} to read, update, or delete every document in the collection.*

Versions of budibase server the record lists as affected:

- 3.39.18 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-2026-137498
```

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-2026-137498
```

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 any configuration change short of upgrading can disable the PUBLIC query feature or restrict access to query endpoints.
- Whether cloud-hosted Budibase instances are affected, or whether this applies only to self-hosted @budibase/server deployments.
- Whether the app ID and query ID are discoverable by an unauthenticated caller without any prior access to the app.
- Whether Budibase 4.0.0 addresses vulnerabilities beyond this prototype pollution flaw.
- 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 27 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-2026-137498: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N` 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	None	No effect on availability.

Appendix 2. Timeline

Date	Event
26 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
Budibase server 3.39.18–3.x with at least one PUBLIC MongoDB query in a published app, reachable over a network	High	Upgrade to 4.0.0 immediately
Same version range; MongoDB datasource present but no query has PUBLIC execution permission	Medium	Upgrade at next patch cycle; confirm no PUBLIC queries exist
Affected version installed; no MongoDB datasource configured in any published app	Low	Upgrade at next patch cycle
Running Budibase 4.0.0 or later on all systems	None	No action needed for this CVE

Budibase server not installed on the estate	None	Nothing to do for this CVE

Appendix 4. Definition of done

- Every budibase server 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-2026-137498: https://www.cve.org/CVERecord?id=CVE-2026-137498
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/Budibase/budibase/security/advisories/GHSA-x4w8: https://github.com/Budibase/budibase/security/advisories/GHSA-x4w8-596q-fmh7
- Advisory or release notes read: www.vulncheck.com/advisories/budibase-server-3.39.18-before-4.0.0: https://www.vulncheck.com/advisories/budibase-server-3.39.18-before-4.0.0-mongodb-filter-erasure-via-proto-keys