contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# Strapi exploited

**CVE-2023-22894 · on CISA's exploited list since 8 October 2026**

## Analysis Report

Anyone running Strapi should confirm the version now, because CISA's date of 11 October 2026 has passed. First find every Strapi install and its version. If you do not run Strapi, you can stop …

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 1 November 2026 |
| FACTS AS OF | 1 November 2026 | VERSION | 1.0 |
| SEVERITY | **High: CVSS 3.1 7.2** | STATUS | On CISA's exploited list; due 11 October 2026 |

**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/strapi-cve-2023-22894

## The bottom line

> *Anyone running Strapi should confirm the version now, because CISA's date of 11 October 2026 has passed. First find every Strapi install and its version. If you do not run Strapi, you can stop reading.*

## At a glance

| Fact | Detail |
|---|---|
| Product | Strapi (CVE-2023-22894) |
| Severity | High: 7.2 (CVSS 3.1) |
| CISA | On its exploited list since 8 October 2026. Deadline for US federal agencies: 11 October 2026. |
| Chance of exploitation (EPSS) | 0.04, the estimated chance in the next 30 days, as at 1 November 2026 |
| Ransomware use | Not recorded by CISA. That is not the same as none. |
| Fixed in | No source we read names a fixed version |
| Who looks first | Anyone running Strapi. The record says 4.5.5 and earlier; a researcher's write-up says up to 4.7.1. The attacker needs admin panel access first. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run Strapi, or does a supplier run it for you (a website, app or portal back end)? | Nothing to do for this CVE. | Find the version (next question). |
| Is it version 4.7.1 or earlier, or Strapi 3? | Ask your provider to confirm in writing; then nothing more for this CVE. | Treat it as affected and plan the upgrade. |
| Can anyone you do not fully trust reach the admin panel, or hold an admin or editor login? | Lower risk, but still upgrade. | Restrict access and review those accounts now. |

## What it is

An attacker who already has access to the Strapi admin panel can filter users by private columns and infer values from the replies. The record says that with super admin access this reveals every user's password hash and password reset token.

## Why it matters

Our reading is that this flaw is a step, not a break-in on its own, because the attacker needs admin panel access first. A stolen reset token or hash could let a low-level account take over a more powerful one. CISA says it can be chained with CVE-2023-22621 to reach remote code execution. The researcher's write-up says the pair hijacks super admin users and then runs code without a login on versions up to 4.5.5. A score of 7.2 undersells that.

## What the vendor's advisory says

We read three pages on strapi.io and github.com and www.ghostccamm.com. In short:

- The vendor's advisory covers CVE-2023-22893, CVE-2023-22621 and CVE-2023-22894 together, published 17 April 2023.
- For CVE-2023-22621 the vendor says versions up to 4.5.5 are affected and 4.5.6 or later fixes it.
- The vendor strongly advises going beyond version 4.8.0, where other security flaws were patched.
- The vendor says Strapi 3 reached end of life on 31 December 2022 and gets no security updates.
- For CVE-2023-22621 only, the vendor has released patch-package patches for those who cannot upgrade.

## Things people will get wrong

- "It needs a login, so it is not urgent." CISA lists it as exploited and says it chains with CVE-2023-22621 for code execution. The login needed may be a low-level admin or editor account.
- "We patched CVE-2023-22621, so we are covered." These are separate flaws. The vendor's fixed version for CVE-2023-22621 is 4.5.6, but the sources here do not name the fixed version for this one.
- "It only leaks usernames." The record says a super admin attacker can discover the password hash and password reset token of all users.

## 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 versions you run

- List every Strapi install, including ones a web agency or supplier hosts for you.
- Note the version of each, and whether the admin panel is reachable from the internet.

```
npm ls @strapi/strapi
```

## Step 2: Reduce exposure to the admin panel

- Limit the admin panel to known networks or a VPN, and remove admin and editor accounts nobody needs.
- Reset passwords for all users if you cannot rule out misuse, because hashes and reset tokens may have been read.

## Step 3: Upgrade

- The sources here do not name a fixed version for this CVE. The vendor advises going beyond 4.8.0, so ask for the newest supported release.
- Move off Strapi 3, which gets no security updates.

## Step 4: Check for signs of misuse

- Review request logs for unusual user queries filtered on private fields.
- Search for a PUT request to the users-permissions email-templates path, which the vendor gives as the sign for CVE-2023-22621, and check the templates for odd code.

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, CISA lists a flaw in Strapi, CVE-2023-22894, as exploited. Please tell us whether we run Strapi anywhere, including services you host for us, and which version each one is. The record says versions up to 4.5.5 are affected, and a write-up says up to 4.7.1. The vendor advises going beyond 4.8.0. Please also tell us who can reach each admin panel. Please confirm in writing the versions found and the upgrade, or your plan for it, by a date you suggest. Thank you.*

## Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Admin logins from unfamiliar addresses, or new admin accounts you did not create.
- Repeated requests to list users with filters on private fields such as password or reset token.
- Password resets nobody asked for, or edits to the email templates.

## The weakness behind it

CISA's entry classes this as CWE-312 (Cleartext Storage of Sensitive Information).

## The sources, in their words

CISA's catalogue entry:

> *Strapi contains a cleartext storage of sensitive information vulnerability that could allow attackers with access to the admin panel to discover sensitive user details via the query filter. The impacted product(s) could be end-of-life (EoL) and/or end-of-service (EoS). Users are advised to discontinue use and/or transition to a supported version. This vulnerability can be chained with CVE-2023-22621 to achieve remote code execution.*

The CVE record, published by Mitre on 19 April 2023:

> *Strapi through 4.5.5 allows attackers (with access to the admin panel) to discover sensitive user details by exploiting the query filter. The attacker can filter users by columns that contain sensitive information and infer a value from API responses. If the attacker has super admin access, then this can be exploited to discover the password hash and password reset token of all users. If the attacker has admin panel access to an account with permission to access the username and email of API users with a lower privileged role (e.g., Editor or Author), then this can be exploited to discover sensitive information for all API users but not other admin accounts.*

The record gives no version ranges. Use the vendor's advisory for the affected versions.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

## What we do not know yet

- Which Strapi version first fixes this CVE; the sources here do not name it.
- Whether the record's 4.5.5 or the write-up's 4.7.1 is the true upper limit.
- How attackers have used it, or how many installs have been hit.
- Whether the admin panel on a typical install is exposed to the internet.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- 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", "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-2023-22894**: score 7.2, `CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

| 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 | High | An administrator 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 |
|---|---|
| 19 April 2023 | CVE record published by Mitre. |
| 8 October 2026 | CISA added it to its list of exploited vulnerabilities. |
| 11 October 2026 | CISA's deadline for US federal agencies. |

## 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 |
|---|---|---|
| Strapi 4.x at or below 4.7.1 with the admin panel reachable from the internet | High | Now; CISA's date has passed |
| Strapi 3.x anywhere | High | Now; move to a supported 4.x or later |
| Affected Strapi with the admin panel limited to a few known staff | Medium | This week |

| | | |
|---|---|---|
| Strapi newer than 4.8.0 | Low | Next patch cycle; confirm the version |
| No Strapi in your estate or your suppliers' services | None | None for this CVE |

## Appendix 4. Definition of done

- Every Strapi you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

## Sources


- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2023-22894: https://www.cve.org/CVERecord?id=CVE-2023-22894
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: strapi.io/blog/security-disclosure-of-vulnerabilities-cve: https://strapi.io/blog/security-disclosure-of-vulnerabilities-cve
- Advisory or release notes read: github.com/strapi/strapi/releases: https://github.com/strapi/strapi/releases
- Advisory or release notes read: www.ghostccamm.com/blog/multi_strapi_vulns/: https://www.ghostccamm.com/blog/multi_strapi_vulns/