

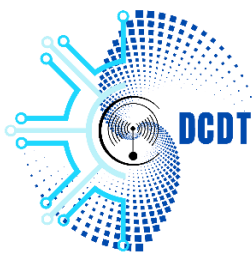
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

9 October 2026

**Advisory 350: Strapi CMS Private Field Filtering Sensitive Data Exposure
Vulnerability - Actively Exploited (CVE-2023-22894).**

Release Date: 8th October 2026

Impact: **HIGH**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2023-22894 is a sensitive information exposure vulnerability (CWE-312) in Strapi, the open-source headless content management system (CMS). Attackers can abuse the query filter to search on private fields of user records, which lets them recover password hashes and password reset tokens, and the usernames and emails of API users. The exploit payload appears in the GET request parameters, for example filters on password, email or resetPasswordToken. A recovered reset token can be used to take over an account, including an administrator account.

What are the systems affected?

The following Strapi versions are affected:

- Strapi 3.2.1 up to, but not including, 4.8.0 (the CVE description itself says through 4.5.5, but the fixed release is 4.8.0)

Not affected / patched version:

- Strapi 4.8.0 or later, released on 15 March 2023. Strapi 3.x will not receive a patch, so Strapi 3 deployments must be migrated to Strapi 4.8.0 or later

What does this mean?

Successful exploitation may allow attackers to:

- Read the password hashes and password reset tokens of users, and the usernames and emails of API users, through crafted filter requests
- Use stolen reset tokens to take over accounts, including administrator accounts, and then change or publish content or reach connected services
- Crack leaked password hashes offline and reuse credentials on other systems

Mitigation process

CERTVU recommends the following:

1. Upgrade Strapi

Upgrade to Strapi 4.8.0 or later, preferably the latest supported release. Migrate any Strapi 3.x deployment, because it will not be patched.

2. Find every Strapi instance

3. Check the logs

4. Reset credentials

5. Reduce exposure

Restrict the Strapi admin panel and API to trusted networks where possible, put a web application firewall in front of internet-facing instances, and report suspected compromise to CERTVU.

Reference

1. <https://medium.com/strapi/security-disclosure-of-vulnerabilities-cve-2023-22893-cve-2023-22621-and-cve-2023-22894-59a9ade86199>
2. <https://nvd.nist.gov/vuln/detail/CVE-2023-22894>
3. <https://app.opencve.io/cve/CVE-2023-22894>
4. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>