kos0ng Update README.md CVE-2022-31367 ... 16 days ago History

..

README.md 16 days ago

exploit.py 16 days ago

README.md

CVE-2022-31367

Vulnerability Explanation

An authenticated user with permission to **read** "user" data in settings section can dump all available users password hash. This vulnerability caused by column name manipulation (column name injection) on filtering feature.

Vulnerability Type

SQL Injection

Attack Vector

An authenticated user with permission to read user data in settings section can dump all users data such as password hash by manipulating column when using filter function

Vendor of Product

Strapi

Affected Version

- Strapi - v3.* . Fixed on v3.6.10
- Strapi - v4.* . Fixed on v4.1.10

Steps to Reproduce

1. Login to user with permission to **read** "user" data in settings section.
2. Click on filters and add filter using **firstname** and **email** with type of selection is **contains case sensitive**
3. See http request and then click edit and send (firefox) . After that change **email_containss** to **password_containss** and fill **password_contains** parameter with "$" , because we know that password in strapi hashed using bcrypt.
4. Check the response and we will see row of data which fulfil our filter request (in this case password contains $ and username contains admin)
5. Validate the bug by sending an invalid filter value such as "JUNK" for **password**.
6. Final step, create script to automate password leak and validate the password found by checking on database.

Exploit Code

- exploit.py

Tested On

- Node.js version: v12.22.7
- NPM version: 7.24.2
- Strapi version: v3.6.8
- Database: PostgreSQL
- Operating system: Debian GNU/Linux 9 (stretch)

Disclosure Timeline:

- 2021-12-09: Vulnerability discovered.
- 2022-05-11: Vulnerability fixed.
- 2022-05-11: Vulnerability reported to the MITRE corporation.
- 2022-05-23: CVE has been assigned.
- 2022-09-27: Public disclosure of the vulnerability.

Discoverer

Achmad Zaenuri Dahlan Putra (kosong)

Reference

- https://github.com/strapi/strapi/releases/tag/v4.1.10
- https://github.com/strapi/strapi/releases/tag/v3.6.10