frame84 update History

1 contributor

55 lines (39 sloc) | 2.52 KB

SQL Injection

Description

Authenticated SQL Injection vulnerability in the statistics page (/statistics/retrieve) of Maarch RM 2.8, via filter parameter, allows the complete disclosure of all databases. It requires specific privilege to access the vulnerable page, /statistics. Affected Products: Maarch RM 2.7-2.8.

Information

- CVE ID: CVE-2022-37773
- Vulnerability Type: SQL Injection (SQLi)
- Vendor of Product: Maarch Xelians
- Affected Product:
  - Maarch RM 2.8.X - all versions < 2.8.6
  - Maarch RM 2.9.X - all versions < 2.9.1
- Affected Component: page: /statistics/retrieve ; parameter: filter
- Editor confirmed: Yes
- Discoverer: François Mehault (francois.mehault -at- proton -dot- me)

References

- Advisory: https://github.com/frame84/vulns
- CVE: CVE-2022-37773
- Product site: https://maarch.ovh/maarch-rm/
- Release advisories:
  - https://labs.maarch.org/maarch/maarchRM/-/blob/Support/2.8.X/CHANGELOG.md
  - https://labs.maarch.org/maarch/maarchRM/-/blob/Support/2.9.X/CHANGELOG.md
- ExploitDB: NA

Approximate Timeline

- 2022/07/22: Vulnerabilities discovered
- 2022/07/29: Vulnerabilities reported to the editor (Maarch Xelians)
- 2022/08/31: Confirmation of vulnerability by the editor
- 2022/10/18: Vendor issued an official fix (Maarch RM 2.8.6 and 2.9.1)

Technical details

SQL Injection - Maarch RM 2.8, /statistics/retreive, filter

- Vulnerable parameter : filter
- Payload : '
- Details : Authenticated with an account having the required privileges to access the statictis page, insert a simple quote in the value of the parameter filter will generate an error sql in the server response. example :
- http://{url}/statistics/retreive?operation=deposit&filter=archivalProfile'&startDate=2022-05-04&endDate=2022-07-23&sizeFilter=1
- Privileges: It require specific privilege to access the vulnerable page, /statics
- Location example: http://{url}/statistics/retreive?filter=

- error generated

```
X-Laabs-Exception: PDOException; SQLSTATE[42601]: Syntax error: 7 ERROR:
unterminated quoted string at or near "',
SUM(CAST(NULLIF("archive_size"."volume", '') AS INTEGER))         FROM
get_children_size "archive_size" INNER JOIN "organization"."organization"
"organization" on "organization"."registrationNumber" =
"archive_size"."org_reg"         GROUP BY "organization"."displayName"" LINE
21: ...CT "organization"."displayName" as archivalProfile', SUM(CAS...
^ in /appli/SAE/src/bundle/Statistics/Controller/Statistics.php:853
```