← CVE Disclosures

Author: Bhaskar Tejaswi (https://users.encs.concordia.ca/~b_tejasw/)
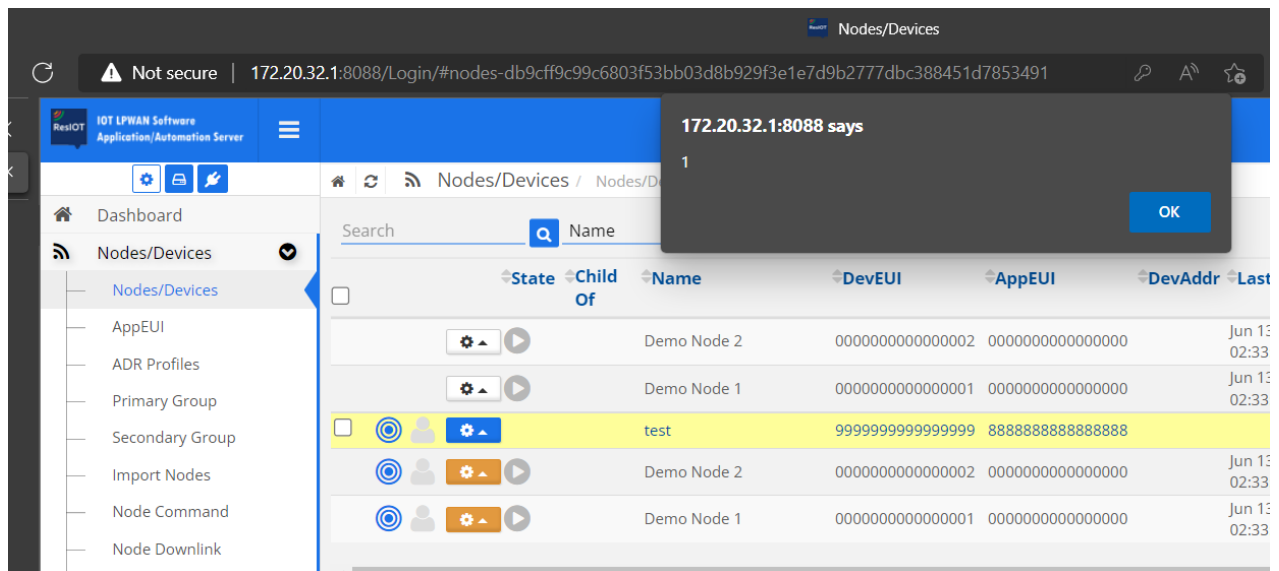
CVE-ID: CVE-2022-34021

October 12, 2022

Multiple Cross Site Scripting (XSS) vulnerabilities in ResIOT IOT Platform + LoRaWAN Network Server through 4.1.1000114 via the form fields.

Upon entering text such as "<script>alert(1)</script>" in form fields, the application stores them and renders them as JavaScript code instead of text.

E.g., XSS in Node Name (test<img src=# onerror=alert(1)>)

References:

https://www.resiot.io/en/changelog/ (Patched Version: 4.1.1000118, Release Date: 31/08/2022)

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_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

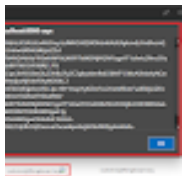## CVE-ID: CVE-2022-35135, CVE-2022-35136

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