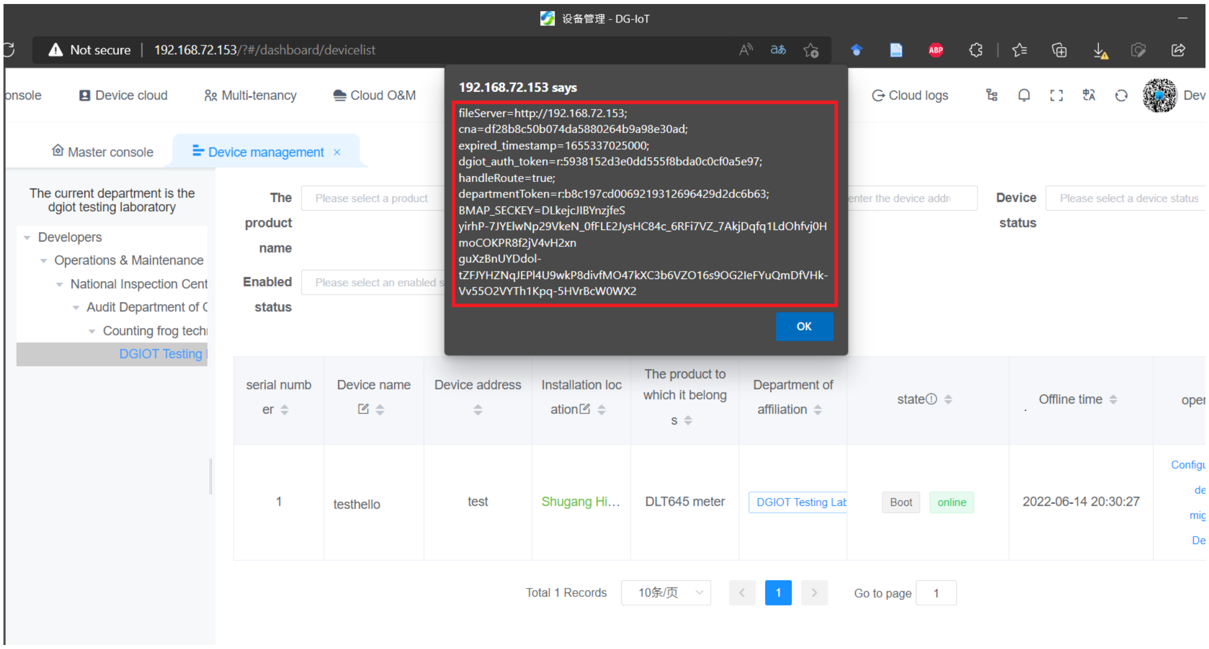
CVE Disclosures

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

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>. These are instances of stored XSS that can be abused to steal admin user cookies.



The product name: Please select a product

Enabled status: Please select an enabled s

enter the device addr

Device status: Please select a device status

192.168.72.153 says

```
fileServer=http://192.168.72.153;
cna=df28b8c50b074da5880264b9a98e30ad;
expired_timestamp=1655337025000;
dgiot_auth_token=r:5938152d3e0dd555f8bda0c0cf0a5e97;
handleRoute=true;
departmentToken=r:b8c197cd0069219312696429d2dc6b63;
BMAP_SECKEY=DLkejcJIBYnzjfeS
yirhP-7JYElwNp29VkeN_0fFLE2JysHC84c_6RFi7VZ_7AkjDqfq1LdOhfvj0H
moCOKPR8f2jV4vH2xn
guXzBnUYDdol-
tZFJYHZNqJEPl4U9wkP8divfMO47kXC3b6VZO16s9OG2IeFYuQmDfVHk-
Vv55O2VYTh1Kpq-5HVrBcW0WX2
```

OK

serial number	Device name	Device address	Installation location	The product to which it belongs	Department of affiliation	state	Offline time	oper
1	testhello	test	Shugang Hi…	DLT645 meter	DGIOT Testing Lab	Boot online	2022-06-14 20:30:27	Configu de mig De

Total 1 Records 10条/页 < 1 > Go to page 1

References:

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

Popular posts from this blog

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

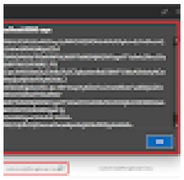
October 12, 2022

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