COMMUNITY CONTENT

Submit #783323: Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Authentication Bypass Issues

Title Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Authentication Bypass Issues

Description Authentication enforcement is performed on the client side rather than the server. By intercepting and modifying HTTP responses, an attacker can bypass authentication.

Bug 1.1 — Config Panel Bypass

Target

http://technostrobe.shiky.demo:58746/Config/index_config.html?idx=1?userId=0002?keyId=NjlhNTAyZjNiNA#StatusPage

Steps to Reproduce

Set up Burp Suite as HTTP proxy
Navigate to the config URL
In Burp's Intercept tab, intercept the POST response to /LoginCB then drop it
Modify the auth result to indicate success
Forward — the full configuration panel renders

Bug 1.2 — Direct Access (No Proxy Needed)

GET /Technostrobe/surveillance_generale.html?idx=1?userId=0002?keyId=NjlhNTAyZjNiNA

This one doesn't even need response manipulation. The server serves the page directly with no authentication check at all. Just visiting the URL works.

Type URL in browser bar
↓
Full surveillance dashboard loads
↓
No login prompt. No session check. Nothing.

Bug 1.3 — Light Control Board Bypass

Target

http://technostrobe.shiky.demo:58746/Technostrobe/surveillance_ctrlboard.html?idx=1?userId=0001?keyId=NjlhNTAyZjNiNA

This is the highest impact instance. The light control board allows:

Changing light flash patterns

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

Toggling lights on/off
Modifying timing sequences

```
┌──────────────────────────────────────────────┐
│        WHAT THE LIGHT CONTROL BOARD CONTROLS │
│                                              │
│  Flash Pattern:   -> can be changed remotely │
│  Flash Rate:      [72 fpm ]  -> FAA requires specific rates
│  Intensity:       [100%   ]  -> day/night levels
│  Sync:            [enabled ] -> multi-tower sync
│                                              │
│  If this is tampered with:                   │
│  - Lights go dark  -> aviation hazard        │
│  - Wrong pattern   -> confuses pilots        │
│  - Sync broken     -> regulatory violation   │
└──────────────────────────────────────────────┘
```

Same bypass method as 1.1: intercept the /LoginCB response and modify it to indicate auth success.

The server does not validate session state for subsequent requests.

Root Cause:

Authentication decisions rely on client-side logic instead of server-side validation.

Impact:

Full authentication bypass

Unauthorized access to admin functionality

No valid credentials required

Source https://github.com/shiky8/my-cve-vulnerability-research/blob/main/my_VulnDB_cves/CVE-TECHNOSTROBE-02-AuthBypass.md

User shiky8 (UID 96565)

Submission 03/20/2026 01:16 AM (17 days ago)

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

Status Pending

VulDB entry [Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30 /LoginCB index_config Improper Authentication]

Points 20

© 1997-2026 vuldb.com · cc by-nc-sa