Submit #563430: TOTOLINK A720R V4.1.5cu.374 Improper Access Controls

Title	TOTOLINK A720R V4.1.5cu.374 Improper Access Controls
Description	The TOTOLINK A720R V4.1.5cu.374 firmware contains an unauthenticated diagnostic log clearing vulnerability. An attacker can exploit this flaw by sending a crafted POST request with the parameter {"topicurl":"clearDiagnosisLog"} to /cgi-bin/cstecgi.cgi, allowing unauthorized clearing of system diagnostic logs without authentication.
Source	⚠ https://github.com/at0de/my_vulns/blob/main/TOTOLINK/A720R/clearDiagnosisLog.md
User	153528990 (UID 64409)
Submission	04/22/2025 03:48 AM (14 days ago)
Moderation	05/04/2025 08:24 PM (13 days later)
Status	Accepted
VulDB Entry	307373 [TOTOLINK A720R 4.1.5cu.374 Log /cgi-bin/cstecgi.cgi topicurl access control]
Points	19

Notice

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