Submit #563444: TOTOLINK A720R V4.1.5cu.374 Exposure of Sensitive System Information to an Unauthorized Cont

Title	TOTOLINK A720R V4.1.5cu.374 Exposure of Sensitive System Information to an Unauthorized Cont
Description	The TOTOLINK A720R V4.1.5cu.374 firmware contains an unauthenticated system log disclosure vulnerability. An attacker can exploit this flaw by sending a crafted POST request with the parameter {"topicurl":"showSyslog"} to /cgi-bin/cstecgi.cgi, exposing detailed system logs containing kernel-level debug information, network interface status changes, wireless configuration details, and low-level hardware operations.
Source	⚠️ https://github.com/at0de/my_vulns/blob/main/TOTOLINK/A720R/showSyslog.md
User	153528990 (UID 64409)
Submission	04/22/2025 04:07 AM (14 days ago)
Moderation	05/04/2025 08:25 PM (13 days later)
Status	Accepted
VulDB Entry	307375 [TOTOLINK A720R 4.1.5cu.374 /cgi-bin/cstecgi.cgi topicurl information disclosure]
Points	20

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