COMMUNITY CONTENT

Home › Submit › 779140

Submit #779140: Totolink A3300R 17.0.0cu.557_b20221024 Command Injection

Title	Totolink A3300R 17.0.0cu.557_b20221024 Command Injection
Description	The vulnerability resides within the router's shttpdservice. It allows a remote attacker to execute arbitrary operating system commands by sending a specially crafted network request. The technical root cause is a command injection flaw in the handling of user input: The attack vector is a user-supplied parameter named enable. The program flow reads this parameter in the sub_41458Cfunction and passes it to Uci_Set_Str. Subsequently, the value of the "enable" parameter is unsafely concatenated into a command string (variable v11) using snprintf. This crafted command string is then passed to the CsteSystemfunction, where it is ultimately executed by the execv()system call, leading to arbitrary command execution.
Source	⚠ https://github.com/LvHongW/Vuln-of-totolink_A3300R/tree/main/A3300R_enable_cmd_inject
User	LvHW (UID 96399)
Submission	03/13/2026 03:25 AM (17 days ago)
Moderation	03/29/2026 07:51 PM (17 days later)
Status	Accepted
VulDB entry	354128 [Totolink A3300R 17.0.0cu.557_b20221024 /cgi-bin/cstecgi.cgi setUPnPCfg enable command injection]
Points	20

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