COMMUNITY CONTENT

Home › Submit › 779142

Submit #779142: Totolink A3300R 17.0.0cu.557_b20221024 Command Injection

Title	Totolink A3300R 17.0.0cu.557_b20221024 Command Injection
Description	The vulnerability exists 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 involves unsafe handling of user input in a function chain: A user-supplied parameter named "ip" is read by the program. This parameter's value is passed to the Uci_Set_Strfunction. Subsequently, the value of "ip" is unsafely concatenated into a command string (variable v11) using snprintf. This crafted command string is then passed to and executed by the CsteSystemfunction via the execv()system call.
Source	⚠ https://github.com/LvHongW/Vuln-of-totolink_A3300R/tree/main/A3300R_ip_cmd_inject
User	LvHW (UID 96399)
Submission	03/13/2026 03:31 AM (17 days ago)
Moderation	03/29/2026 07:51 PM (17 days later)
Status	Accepted
VulDB entry	354129 [Totolink A3300R 17.0.0cu.557_b20221024 /cgi-bin/cstecgi.cgi setStaticRoute ip 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