COMMUNITY CONTENT

Submit #773727: Tenda A18pro V02.03.02.28 Stack-based Buffer Overflow

Title	Tenda A18pro V02.03.02.28 Stack-based Buffer Overflow
Description	During a security review of the Tenda A18pro router firmware (version V02.03.02.28), a critical stack-based buffer overflow vulnerability was identified in the MAC filtering configuration endpoint /goform/setMacFilterCfg. The vulnerability resides in the sub_423B50 function (responsible for parsing MAC filter rules). This function is triggered when a user submits a configuration request via the deviceList parameter. The function uses strchr to locate a carriage return character (\r, ASCII 13) within the user-provided string. Once found, it employs the unsafe strcpy function to copy the split substrings into a fixed-size stack buffer v15 (160 bytes). Since the length of the input strings is not validated before the copy operation, an attacker can provide a specially crafted long string to overwrite the stack frame, including the return address, leading to a Denial of Service (DoS) or potential Remote Code Execution (RCE).
Source	https://github.com/lilukun337/cve/issues/5
User	lilukun (UID 96152)
Submission	03/06/2026 07:20 AM (1 month ago)
Moderation	03/20/2026 09:33 AM (14 days later)
Status	Published
VulDB entry	[Tenda A18 Pro 02.03.02.28 MAC Filtering Configuration Endpoint /goform/setMacFilterCfg sub_423B50 deviceList stack-based overflow]
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