COMMUNITY CONTENT

Home › Submit › 765330

Submit #765330: Tenda FH451 V1.0.0.9 Stack-based Buffer Overflow

Title	Tenda FH451 V1.0.0.9 Stack-based Buffer Overflow
Description	A vulnerability was found in Tenda FH451 V1.0.0.9. Affected by this vulnerability is the function fromAdvSetWan of the file /goform/AdvSetWan of the component httpd. The manipulation of the argument wanmode and PPPOEPassword with an unknown input leads to a buffer overflow vulnerability.If the value of argument wanmode is 2, the variable v17 is passed to the sub_3C434 function without any length check, which may overflow the stack-based buffer s.
Source	https://github.com/Litengzheng/vul_db/blob/main/FH451/vul_62/README.md
User	LitzHuster (UID 95786)
Submission	02/22/2026 06:26 AM (1 month ago)
Moderation	03/06/2026 10:22 PM (13 days later)
Status	Accepted
VulDB entry	[Tenda FH451 1.0.0.9 /goform/AdvSetWan sub_3C434 wanmode/PPPOEPassword 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