COMMUNITY CONTENT

Home › Submit › 779127

Submit #779127: Tenda FH1201 1.2.0.14(408) Stack-based Buffer Overflow

Title	Tenda FH1201 1.2.0.14(408) Stack-based Buffer Overflow
Description	A vulnerability was found in Tenda FH1201 V1.2.0.14(408) . Affected by this vulnerability is the function formWrlExtraSet of the file /goform/WrlExtraSet of the component httpd. The manipulation of the argument GO with an unknown input leads to a buffer overflow vulnerability.In formWrlExtraSet function,it reads in a user-provided parameter GO.And the variable s is passed to the ask_to_reboot function without any length check, which may overflow the stack-based buffer s_1 by sprintf function.As a result, by requesting the page, an attacker can easily execute a denial of service attack or remote code execution.
Source	https://github.com/LItengzheng/vul_db/blob/main/FH1201/vul_44/README.md
User	LiZHuster2 (UID 96397)
Submission	03/13/2026 02:35 AM (17 days ago)
Moderation	03/27/2026 05:38 PM (15 days later)
Status	Accepted
VulDB entry	[Tenda FH1201 1.2.0.14(408) Parameter /goform/WrlExtraSet formWrlExtraSet GO 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