COMMUNITY CONTENT

Submit #766932: Tenda F453 v1.0.0.3 Stack-based Buffer Overflow

Title	Tenda F453 v1.0.0.3 Stack-based Buffer Overflow
Description	A vulnerability was found in Tenda F453 v1.0.0.3. Affected by this vulnerability is the function formQuickIndex of the file /goform/QuickIndex of the component httpd. The manipulation of the argument mit_linktype and PPPOEPassword with an unknown input leads to a buffer overflow vulnerability.In formQuickIndex function,it reads in a user-provided parameter mit_linktype and PPPOEPassword.If the value of mit_linktype is 2, the variable v10 is passed to the sub_3C6C0() function without any length check, which may overflow the stack-based buffer s.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/F453/vul_96/README.md
User	LtzHust (UID 95660)
Submission	02/25/2026 12:42 AM (1 month ago)
Moderation	03/07/2026 06:44 PM (11 days later)
Status	Accepted
VulDB entry	349705 [Tenda F453 1.0.0.3 /goform/QuickIndex sub_3C6C0 mit_linktype/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