



Home > Submit > 780208

Submit #780208: Tenda CH22 V1.0.0.1 Stack-based Buffer Overflow

Title Tenda CH22 V1.0.0.1 Stack-based Buffer Overflow

Description A vulnerability was found in Tenda CH22 V1.0.0.1. 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 v8 is passed to the sub_3B698 function without any length check, which may overflow the stack-based buffer s.

Source https://github.com/Litengzheng/vuldb_new/blob/main/CH22/vul_46/README.md

User LtzHust2 (UID 95662)

Submission 03/14/2026 02:53 PM (16 days ago)

Moderation 03/30/2026 03:33 PM (16 days later)

Status Accepted

VulDB entry 354188 [Tenda CH22 1.0.0.1 Parameter /goform/QuickIndex formQuickIndex mit_linktype 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](#)