COMMUNITY CONTENT

Submit #766934: 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 fromPptpUserAdd of the file /goform/PPTPDClient of the component httpd. The manipulation of the argument username and opttype with an unknown input leads to a buffer overflow vulnerability.In fromPptpUserAdd function,it reads in a user-provided parameter username and opttype.If the value of opttype is 1, the variable v21 will be passed to the sprintf function without any length check, which may overflow the stack-based buffer s__3.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_98/README.md
User	LiZHust (UID 95660)
Submission	02/25/2026 12:45 AM (1 month ago)
Moderation	03/07/2026 06:44 PM (11 days later)
Status	Accepted
VulDB entry	350112 [Tenda F453 1.0.0.3/3.As /goform/PPTPDClient fromPptpUserAdd username/opttype 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