



Home > Submit > 768296

Submit #768296: 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 formWrIExtraSet of the file /goform/WrIExtraSet of the component httpd. The manipulation of the argument GO with an unknown input leads to a buffer overflow vulnerability. In formWrIExtraSet function, it reads in a user-provided parameter GO. And the variable v51 is passed to the sub_3A7D8 function without any length check, which may overflow the stack-based buffer s_ 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/F453/vul_69/README.md

User LtzHust2 (UID 95662)

Submission 02/26/2026 06:20 PM (1 month ago)

Moderation 03/07/2026 09:55 PM (9 days later)

Status Accepted

VulDB entry 349746 [Tenda F453 1.0.0.3 /goform/WrIExtraSet formWrIExtraSet 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](#)