



Home > Submit > 774342

Submit #774342: Tenda FH451 V1.0.0.9 Stack-based Buffer Overflow

Title Tenda FH451 V1.0.0.9 Stack-based Buffer Overflow

Description A vulnerability was found in Tenda FH451 V1.0.0.9. 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_3A54C` 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/FH451/vul_41/README.md

User LtzHuster (UID 95786)

Submission 03/07/2026 12:32 AM (1 month ago)

Moderation 03/21/2026 09:05 AM (14 days later)

Status Accepted

VulDB entry 302322 [Tenda FH451 1.0.0.9 /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](#)