

[Home](#) > [Submit](#) > [769463](#)

Submit #769463: Tenda i12 V1.0.0.6(2204) Buffer Overflow

Title Tenda i12 V1.0.0.6(2204) Buffer Overflow

Description We found an overflow vulnerability in httpd :

In formWifiMacFilterGet function,it reads in a user-provided parameter wl_radio and index.

If the value of wl_radio is not 0, the variable Var 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/Jimi-Lab/cve/issues/2>

User Jimi (UID 68862)

Submission 02/28/2026 02:37 AM (1 month ago)

Moderation 03/12/2026 09:30 AM (12 days later)

Status Accepted

VulDB entry 350654 [Tenda i12 1.0.0.6(2204) /goform/WifiMacFilterGet formWifiMacFilterGet index 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](#)