COMMUNITY CONTENT

Submit #785337: Tenda i12 V1.0.0.11(3862) Stack-based Buffer Overflow

Title	Tenda i12 V1.0.0.11(3862) Stack-based Buffer Overflow
Description	A vulnerability identified as critical has been detected in Tenda i12 V1.0.0.11(3862). This impacts the function formwrlSSIDset of the file /goform/wifiSSIDset of the component httpd. Performing a manipulation of the argument wl_radio and index results in stack-based overflow. In formwrlSSIDset function,it reads in a user-provided parameter index and wl_radio.If the value of wl_radio is 0, the variable v22 will be passed to the sprintf function without any length check, which may overflow the stack-based buffer s__2.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/vuldb_new/blob/main/I12/vul_107/README.md
User	LiZHust (UID 95660)
Submission	03/21/2026 11:06 PM (15 days ago)
Moderation	04/05/2026 05:25 PM (15 days later)
Status	Accepted
VulDB entry	[Tenda i12 1.0.0.11(3862) Parameter /goform/wifiSSIDset formwrlSSIDset index/wl_radio 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