COMMUNITY CONTENT

Home › Submit › 768997

Submit #768997: Tenda i3 V1.0.0.6(2204) Buffer Overflow

Title	Tenda i3 V1.0.0.6(2204) Buffer Overflow
Description	Affected component(s): httpd, formwrlSSIDset, /goform/wifiSSIDset, GO Attack vector(s): Remote exploitation via crafted HTTP POST to /goform/wifiSSIDset with an overly long GO parameter. Suggested description: Tenda i3 V1.0.0.6(2204) contains a stack-based buffer overflow in httpd due to insufficient length validation of the GO parameter in formwrlSSIDset. A remote attacker can send a crafted request to /goform/wifiSSIDset to trigger a denial of service or potentially achieve code execution. Discoverer(s)/Credits: Svigo, Huazhong University of Science and Technology
Source	⚠ https://github.com/Svigo-o/Tenda_vul/tree/main/tenda-i3-formwrlSSIDset-go-buffer-overflow
User	Svigo (UID 95964)
Submission	02/27/2026 09:23 AM (1 month ago)
Moderation	03/11/2026 02:52 PM (12 days later)
Status	Duplicate
VulDB entry	359408 [Tenda i3 1.0.0.6(2204) /goform/wifiSSIDset formwrlSSIDset index/GO stack-based overflow]
Points	0

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