



Home > Submit > 768980

Submit #768980: Tenda i3 V1.0.0.6(2204) Buffer Overflow

| | |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title | Tenda i3 V1.0.0.6(2204) Buffer Overflow |
| Description | <p>Affected component(s): httpd, formSetAutoPing, /goform/setAutoPing, ping1</p> <p>Attack vector(s): Remote exploitation via crafted HTTP POST to /goform/setAutoPing with an overly long ping1</p> <p>Suggested description: Tenda i3 V1.0.0.6(2204) contains a stack-based buffer overflow in httpd due to insufficient length validation of the ping1 parameter in formSetAutoPing. A remote attacker can send a crafted request to /goform/setAutoPing to trigger a denial of service or potentially achieve code execution.</p> <p>Discoverer(s)/Credits: Svigo, Huazhong University of Science and Technology</p> |
| Source | https://github.com/Svigo-o/Tenda_vul/tree/main/tenda-i3-setautoping-ping1-buffer-overflow |
| User | Svigo (UID 95964) |
| Submission | 02/27/2026 09:17 AM (1 month ago) |
| Moderation | 03/08/2026 01:39 PM (9 days later) |
| Status | Verified |
| VulDB entry | VUL-2026-0000 [Tenda i3 1.0.0.6(2204) /goform/setAutoPing formSetAutoPing ping1/ping2 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](#)