



Home > Submit > 773670

# Submit #773670: Tenda A18pro V02.03.02.28 Stack-based Buffer Overflow

**Title** Tenda A18pro V02.03.02.28 Stack-based Buffer Overflow

**Description** During a security review of the Tenda A18pro router firmware (version V02.03.02.28), a critical buffer overflow vulnerability was identified in the Wi-Fi schedule configuration endpoint /goform/openSchedWifi.

The vulnerability exists within the setSchedWifi function. This function retrieves user-controlled parameters schedStartTime and schedEndTime via the websGetVar interface. These values are subsequently copied into a heap-allocated buffer of fixed size (25 bytes) using the unsafe strcpy function. Since there is no length validation on the input, an attacker can provide an oversized string to overflow the buffer, leading to memory corruption, Denial of Service (DoS), or potential arbitrary code execution.

**Source** <https://github.com/lilukun337/cve/issues/2>

**User** lilukun (UID 96162)

**Submission** 03/06/2026 06:55 AM (1 month ago)

**Moderation** 03/20/2026 09:33 AM (14 days later)

**Status** Accepted

**VulDB entry** 302018 [Tenda A18 Pro 02.03.02.28 /goform/openSchedWifi setSchedWifi 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](#)