COMMUNITY CONTENT

Submit #782297: Tenda AC10 V4 US_AC10V4.0si_V16.03.10.10_multi_TDE01 Stack-based Buffer Overflow

Title	Tenda AC10 V4 US_AC10V4.0si_V16.03.10.10_multi_TDE01 Stack-based Buffer Overflow
Description	A stack-based buffer overflow vulnerability exists in the fromSysToolChangePwd function (0x004b428c) in /bin/httpd of Tenda AC10 V4 firmware V16.03.10.10. A 36-byte stack buffer (local_2c) is used as the destination for GetValue("sys.userpass", local_2c) without bounds checking. The saved return address is reachable with approximately 48 bytes of overflow. If an oversized value is stored in the sys.userpass NVRAM key via another attack vector, the saved return address can be overwritten enabling arbitrary code execution. The binary lacks stack canaries and PIE protection.
Source	⚠ https://github.com/somanyerrors/tenda-ac10v4-vulnerabilities/blob/main/findings/CRITICAL-04-stackoverflow-fromsystoolchangepwd.md
User	CoreNode (UID 96566)
Submission	03/18/2026 04:32 PM (18 days ago)
Moderation	04/04/2026 03:28 PM (17 days later)
Status	Accepted
VulDB entry	353112 [Tenda AC10 16.03.10.10_multi_TDE01 /bin/httpd fromSysToolChangePwd sys.userpass 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