COMMUNITY CONTENT

Submit #777394: Tenda AC5 AC5 V1.0 V15.03.06.47 Buffer Overflow

Title	Tenda AC5 AC5 V1.0 V15.03.06.47 Buffer Overflow
Description	The Tenda AC5 V1.0 V15.03.06.47 firmware has a stack overflow vulnerability located in the fromWizardHandle function. This function accepts the WANTand WANS parameter from a POST request. Within case 2, this function accepts the PPW parameter from a POST request, which is assigned to decodePwd(pppoepwd, decode_pwd);. However, since the user has control over the input of PPW, the function decodePwd() leads to a buffer overflow. The user-supplied PPW can exceed the capacity of the decode_pwd array, thus triggering this security vulnerability.
Source	https://lavender-bicycle-a5a.notion.site/Tenda_AC5_WizardHandle_PPW-32053a41781f80cab094d750d30dc9a8?source=copy_link
User	wxhwxhwxh_mie (UID 66748)
Submission	03/11/2026 06:46 AM (28 days ago)
Moderation	03/26/2026 04:58 PM (15 days later)
Status	Accepted
VulDB entry	[Tenda AC5 15.03.06.47 POST Request /goform/WizardHandle decodePwd WANT/WANS stack-based overflow]
Points	17

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