VDB-353657 · CVE-2026-4906 · EUVD-2026-16524

# TENDA AC5 15.03.06.47 POST REQUEST /GOFORM/WIZARDHANDLE DECODEPWD WANT/WANS STACK-BASED OVERFLOW

| CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score |
| --- | --- | --- |
| 8.0 | $0-$5k | 0.00 |

## Summary

A vulnerability has been found in Tenda AC5 15.03.06.47 and classified as critical. The impacted element is the function `decodePwd` of the file */goform/WizardHandle* of the component *POST Request Handler*. The manipulation of the argument *WANT/WANS* leads to stack-based overflow. This vulnerability is uniquely identified as CVE-2026-4906. The attack is possible to be carried out remotely. Moreover, an exploit is present.

## Details

A vulnerability, which was classified as critical, has been found in Tenda AC5 15.03.06.47. This issue affects the function `decodePwd` of the file */goform/WizardHandle* of the component *POST Request Handler*. The manipulation of the argument `WANT/WANS` with an unknown input leads to a stack-based overflow vulnerability. Using CWE to declare the problem leads to CWE-121. A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). Impacted is confidentiality, integrity, and availability.

The advisory is shared at lavender-bicycle-a5a.notion.site. The identification of this vulnerability is CVE-2026-4906. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known.

The exploit is available at lavender-bicycle-a5a.notion.site. It is declared as proof-of-concept.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-16524). The entries VDB-261990, VDB-316737, VDB-326203 and VDB-353837 are pretty similar.

## Product

**Type**

- Router Operating System

**Vendor**

- Tenda

**Name**

- AC5

**Version**

- 15.03.06.47

**License**

- commercial

**Website**

- Vendor: https://www.tenda.com.cn/

## CPE 2.3

- 🔒
- 🔒

## CPE 2.2

- 🔒
- 🔒

## CVSSv4

**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

## CVSSv3

**VulDB Meta Base Score**: 8.8
**VulDB Meta Temp Score**: 8.0

**VulDB Base Score**: 8.8
**VulDB Temp Score**: 8.0

**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

## CVSSv2

**VulDB Base Score**: 🔒
**VulDB Temp Score**: 🔒
**VulDB Reliability**: 🔍

## Exploiting

**Class**: Stack-based overflow
**CWE**: CWE-121 / CWE-119
**CAPEC**: 🔒
**ATT&CK**: 🔒

**Physical**: No
**Local**: No
**Remote**: Yes

**Availability**: 🔒
**Access**: Public
**Status**: Proof-of-Concept
**Download**: 🔒

**EPSS Score**: 🔒
**EPSS Percentile**: 🔒

**Price Prediction**: 🔍
**Current Price Estimation**: 🔒

## Threat Intelligence

**Interest**: 🔍
**Active Actors**: 🔍
**Active APT Groups**: 🔍

## Countermeasures

**Recommended**: no mitigation known
**Status**: 🔍

**0-Day Time**: 🔒

## Timeline

| | | |
|---|---|---|
| **03/26/2026** | | Advisory disclosed |
| **03/26/2026** | +0 days | VulDB entry created |
| **03/27/2026** | +1 days | VulDB entry last update |

## Sources

**Vendor**: tenda.com.cn

**Advisory**: lavender-bicycle-a5a.notion.site
**Status**: Not defined

**CVE**: CVE-2026-4906 (🔒)
**GCVE (CVE)**: GCVE-0-2026-4906
**GCVE (VulDB)**: GCVE-100-353657
**EUVD**: 🔒
**scip Labs**: https://www.scip.ch/en/?labs.20161013
**See also**: 🔒

## Entry

**Created**: 03/26/2026 05:03 PM
**Updated**: 03/27/2026 04:28 AM
**Changes**: 03/26/2026 05:03 PM (58), 03/27/2026 04:28 AM (1)
**Complete**: 🔍
**Submitter**: wxhwxhwxh_mie
**Cache ID**: 172:BF8:179

## Submit

**Accepted**

- Submit #777394: Tenda AC5 AC5 V1.0 V15.03.06.47 Buffer Overflow (by wxhwxhwxh_mie)

## Discussion

No comments yet. Languages: en.

Please log in to comment.