



VDB-353656 · CVE-2026-4905 · EUVD-2026-16476

TENDA AC5 15.03.06.47 POST REQUEST /GOFORM/WIFIWPSOOB FORMWIFIWPSOOB INDEX STACK-BASED OVERFLOW

CVSS Meta Temp Score

8.0

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

0.11

Summary

A vulnerability, which was classified as **critical**, was found in **Tenda AC5 15.03.06.47**. The affected element is the function `formWifiWpsOOB` of the file `/goform/WifiWpsOOB` of the component *POST Request Handler*. Executing a manipulation of the argument `index` can lead to stack-based overflow. This vulnerability is handled as **CVE-2026-4905**. The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability classified as **critical** was found in **Tenda AC5 15.03.06.47**. This vulnerability affects the function `formWifiWpsOOB` of the file `/goform/WifiWpsOOB` of the component *POST Request Handler*. The manipulation of the argument `index` with an unknown input leads to a stack-based overflow vulnerability. The CWE definition for the vulnerability is **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). As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared for download at lavender-bicycle-a5a.notion.site. This vulnerability was named **CVE-2026-4905**. The exploitation appears to be easy. The attack can be initiated remotely. Technical details and also a public exploit are known.

It is possible to download the exploit 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-2026-16476**). Entries connected to this vulnerability are available at [VDB-207256](#), [VDB-214113](#), [VDB-252131](#) and [VDB-257665](#).

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-2026-4905](#) (🔒)

GCVE (CVE): [GCVE-0-2026-4905](#)

GCVE (VulDB): [GCVE-100-353656](#)

EUVD: 🔒

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🔒

Entry

Created: 03/26/2026 05:03 PM

Updated: 03/27/2026 02:43 AM

Changes: 03/26/2026 05:03 PM (58), 03/27/2026 02:43 AM (1)

Complete: 🔍

Submitter: [wxhwxhwxh_mie](#)

Cache ID: 20:853:179

Submit

Accepted

- [Submit #777393](#): 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.](#)