VDB-353655 · CVE-2026-4904 · EUVD-2026-16474

TENDA AC5 15.03.06.47 POST REQUEST /GOFORM/SETCFM FORMSETCFM FUNCPARA1 STACK-BASED OVERFLOW

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

Summary

A vulnerability, which was classified as critical, has been found in Tenda AC5 15.03.06.47. Impacted is the function `formSetCfm` of the file */goform/setcfm* of the component *POST Request Handler*. Performing a manipulation of the argument *funcpara1* results in stack-based overflow. This vulnerability is known as CVE-2026-4904. Remote exploitation of the attack is possible. Furthermore, an exploit is available.

Details

A vulnerability classified as critical has been found in Tenda AC5 15.03.06.47. This affects the function `formSetCfm` of the file */goform/setcfm* of the component *POST Request Handler*. The manipulation of the argument `funcpara1` with an unknown input leads to a stack-based overflow vulnerability. CWE is classifying the issue as 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). This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at lavender-bicycle-a5a.notion.site. This vulnerability is uniquely identified as CVE-2026-4904. The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details and a public exploit are known.

The exploit is shared for download 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-2026-16474). Similar entries are available at VDB-307402, VDB-314439, VDB-320839 and VDB-325036.

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-2026-4904 (🔒)
GCVE (CVE): GCVE-0-2026-4904
GCVE (VulDB): GCVE-100-353655
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: 52:576:179

Submit

Accepted

- Submit #777381: 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.