VDB-352402 · CVE-2026-4565 · EUVD-2026-14343

TENDA AC21 16.03.08.16 SETNETCONTROLLIST FORMSETQOSBAND LIST BUFFER OVERFLOW

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

Summary

A vulnerability categorized as critical has been discovered in Tenda AC21 16.03.08.16. The affected element is the function `formSetQosBand` of the file */goform/SetNetControlList*. Executing a manipulation of the argument *list* can lead to buffer overflow. This vulnerability is tracked as CVE-2026-4565. The attack can be launched remotely. Moreover, an exploit is present.

Details

A vulnerability was found in Tenda AC21 16.03.08.16. It has been declared as critical. This vulnerability affects the function `formSetQosBand` of the file */goform/SetNetControlList*. The manipulation of the argument `list` with an unknown input leads to a buffer overflow vulnerability. The CWE definition for the vulnerability is CWE-120. The product copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability was named CVE-2026-4565. 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 github.com. 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-2026-14343). The entries VDB-249710, VDB-256896, VDB-257456 and VDB-257937 are pretty similar.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- AC21

Version

- 16.03.08.16

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: Buffer overflow
CWE: CWE-120 / 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

03/22/2026		Advisory disclosed
03/22/2026	+0 days	VulDB entry created
03/23/2026	+1 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-4565 (🔒)
GCVE (CVE): GCVE-0-2026-4565
GCVE (VulDB): GCVE-100-352402
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/22/2026 09:34 AM
Updated: 03/23/2026 06:46 AM
Changes: 03/22/2026 09:34 AM (57), 03/23/2026 06:46 AM (1)
Complete: 🔍
Submitter: junqi
Cache ID: 128:219:179

Submit

Accepted

- Submit #775119: Tenda AC21 Tenda AC21 V1.0 V16.03.08.16 Buffer Overflow (by junqi)

Discussion

No comments yet. Languages: en.

Please log in to comment.