VDB-351210 · CVE-2026-4252 · GCVE-100-351210

TENDA AC8 16.03.50.11 IPV6 CHECK_IS_IPV6 IP ADDRESS FOR AUTHENTICATION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
9.2	$0-$5k	0.00

Summary

A vulnerability was found in Tenda AC8 16.03.50.11. It has been declared as critical. This affects the function `check_is_ipv6` of the component *IPv6 Handler*. The manipulation results in ip address for authentication. This vulnerability is known as CVE-2026-4252. It is possible to launch the attack remotely. Furthermore, an exploit is available. Applying restrictive firewalling is recommended.

Details

A vulnerability, which was classified as critical, was found in Tenda AC8 16.03.50.11. Affected is the function `check_is_ipv6` of the component *IPv6 Handler*. The manipulation with an unknown input leads to a ip address for authentication vulnerability. CWE is classifying the issue as CWE-291. The product uses an IP address for authentication. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is traded as CVE-2026-4252. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known.

The exploit is shared for download at github.com. It is declared as proof-of-concept.

It is possible to mitigate the weakness by firewalling .

Similar entries are available at VDB-211021, VDB-211090, VDB-215242 and VDB-230456.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- AC8

Version

- 16.03.50.11

License

- commercial

Website

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

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 9.8
VulDB Meta Temp Score: 9.2

VulDB Base Score: 9.8
VulDB Temp Score: 8.6
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 9.8
CNA Vector: 🔒

CVSSv2

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

Exploiting

Class: Ip address for authentication
CWE: CWE-291 / CWE-287
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Programming Language: 🔒
Download: 🔒

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: Firewall
Status: 🔍

0-Day Time: 🔒

Timeline

03/16/2026		Advisory disclosed
03/16/2026	+0 days	VulDB entry created
03/21/2026	+5 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-4252 (🔒)
GCVE (CVE): GCVE-0-2026-4252
GCVE (VulDB): GCVE-100-351210
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/16/2026 07:21 AM
Updated: 03/21/2026 01:41 PM
Changes: 03/16/2026 07:21 AM (57), 03/21/2026 01:41 PM (32)
Complete: 🔍
Submitter: DigitalAndrew
Cache ID: 74:9D5:179

Submit

Accepted

- Submit #771759: Tenda AC8 V5 V16.03.50.11 Authentication Bypass Issues (by DigitalAndrew)

Discussion

No comments yet. Languages: en.

Please log in to comment.