VDB-350654 · CVE-2026-4042 · GCVE-100-350654

# TENDA I12 1.0.0.6(2204) /GOFORM/WIFIMACFILTERGET FORMWIFIMACFILTERGET INDEX STACK-BASED OVERFLOW

| CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score |
|---|---|---|
| 8.4 | $0-$5k | 0.22 |

## Summary

A vulnerability labeled as critical has been found in Tenda i12 1.0.0.6(2204). The impacted element is the function `formWifiMacFilterGet` of the file */goform/WifiMacFilterGet*. Such manipulation of the argument *index* leads to stack-based overflow. This vulnerability is traded as CVE-2026-4042. The attack may be launched remotely. Furthermore, there is an exploit available.

## Details

A vulnerability was found in Tenda i12 1.0.0.6(2204) and classified as critical. Affected by this issue is the function `formWifiMacFilterGet` of the file */goform/WifiMacFilterGet*. The manipulation of the argument `index` 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 available at github.com. This vulnerability is handled as CVE-2026-4042. The exploitation is known to be easy. The attack may be launched remotely. Technical details as well as a public exploit are known.

The exploit is available 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 entries VDB-206267, VDB-209510, VDB-214705 and VDB-215147 are related to this item.

## Product

**Type**

- Router Operating System

**Vendor**

- Tenda

**Name**

- i12

**Version**

- 1.0.0.6(2204)

**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**: 8.8
**VulDB Meta Temp Score**: 8.4

**VulDB Base Score**: 8.8
**VulDB Temp Score**: 8.0
**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

**CNA Base Score**: 8.8
**CNA Vector**: 🔒

## 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

| | | |
|---|---|---|
| **03/12/2026** | | Advisory disclosed |
| **03/12/2026** | +0 days | VulDB entry created |
| **03/17/2026** | +5 days | VulDB entry last update |

## Sources

**Vendor**: tenda.com.cn

**Advisory**: github.com
**Status**: Not defined

**CVE**: CVE-2026-4042 (🔒)
**GCVE (CVE)**: GCVE-0-2026-4042
**GCVE (VulDB)**: GCVE-100-350654
**scip Labs**: https://www.scip.ch/en/?labs.20161013
**See also**: 🔒

## Entry

**Created**: 03/12/2026 09:35 AM
**Updated**: 03/17/2026 11:38 AM
**Changes**: 03/12/2026 09:35 AM (57), 03/17/2026 11:38 AM (32)
**Complete**: 🔍
**Submitter**: Jimi
**Cache ID**: 172:194:179

## Submit

### Accepted

- Submit #769463: Tenda i12 V1.0.0.6(2204) Buffer Overflow (by Jimi)

### Duplicate

- [redacted]

## Discussion

No comments yet. Languages: en.

Please log in to comment.