VDB-350655 · CVE-2026-4043 · GCVE-100-350655

TENDA I12 1.0.0.6(2204) /GOFORM/WIFISSIDGET FORMWRLSSIDGET INDEX STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	0.22

Summary

A vulnerability marked as critical has been reported in Tenda i12 1.0.0.6(2204). This affects the function `formwrlSSIDget` of the file */goform/wifiSSIDget*. Performing a manipulation of the argument *index* results in stack-based overflow. This vulnerability is known as CVE-2026-4043. Remote exploitation of the attack is possible. Furthermore, an exploit is available.

Details

A vulnerability was found in Tenda i12 1.0.0.6(2204). It has been classified as critical. This affects the function `formwrlSSIDget` of the file */goform/wifiSSIDget*. The manipulation of the argument `index` 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 github.com. This vulnerability is uniquely identified as CVE-2026-4043. 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 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.

Similar entries are available at VDB-206266, VDB-209509, VDB-214704 and VDB-246459.

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: 🔍

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

03/12/2026		Advisory disclosed
03/12/2026	+0 days	VulDB entry created
03/12/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-4043 (🔒)
GCVE (CVE): GCVE-0-2026-4043
GCVE (VulDB): GCVE-100-350655
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/12/2026 09:35 AM
Changes: 03/12/2026 09:35 AM (57)
Complete: 🔍
Submitter: Jimi
Cache ID: 4:913:179

Submit

Accepted

- Submit #769464: Tenda i12 V1.0.0.6(2204) Buffer Overflow (by Jimi)

Duplicate

- [redacted]

Discussion

No comments yet. Languages: en.

Please log in to comment.