VDB-355400 · CVE-2026-5609 · GCVE-100-355400

TENDA I12 1.0.0.11(3862) PARAMETER /GOFORM/WIFISSIDSET FORMWRLSSIDSET INDEX/WL_RADIO STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	3.24-

Summary

A vulnerability labeled as critical has been found in Tenda i12 1.0.0.11(3862). Affected by this issue is the function `formwrlSSIDset` of the file */goform/wifiSSIDset* of the component *Parameter Handler*. Such manipulation of the argument *index/wl_radio* leads to stack-based overflow. This vulnerability is referenced as CVE-2026-5609. It is possible to launch the attack remotely. Furthermore, an exploit is available.

Details

A vulnerability was found in Tenda i12 1.0.0.11(3862). It has been rated as critical. Affected by this issue is the function `formwrlSSIDset` of the file */goform/wifiSSIDset* of the component *Parameter Handler*. The manipulation of the argument `index/wl_radio` 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 shared for download at github.com. This vulnerability is handled as CVE-2026-5609. 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.

Similar entries are available at VDB-209507, VDB-215148, VDB-216397 and VDB-252257.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- i12

Version

- 1.0.0.11(3862)

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: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5609 (🔒)
GCVE (CVE): GCVE-0-2026-5609
GCVE (VulDB): GCVE-100-355400
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 05:30 PM
Changes: 04/05/2026 05:30 PM (58)
Complete: 🔍
Submitter: LtzHust
Cache ID: 64:ED1:179

Submit

Accepted

- Submit #785337: Tenda i12 V1.0.0.11(3862) Stack-based Buffer Overflow (by LtzHust)

Discussion

No comments yet. Languages: en.

Please log in to comment.