VDB-350411 · CVE-2026-3976 · EUVD-2026-11517

TENDA W3 1.0.0.3(2204) POST PARAMETER /GOFORM/WIFIMACFILTERSET FORMWIFIMACFILTERSET INDEX/GO STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.56

Summary

A vulnerability was found in Tenda W3 1.0.0.3(2204). It has been classified as critical. The affected element is the function `formWifiMacFilterSet` of the file */goform/WifiMacFilterSet* of the component *POST Parameter Handler*. The manipulation of the argument *index/GO* leads to stack-based overflow. This vulnerability is documented as CVE-2026-3976. The attack can be initiated remotely. Additionally, an exploit exists.

Details

A vulnerability was found in Tenda W3 1.0.0.3(2204) and classified as critical. This issue affects the function `formWifiMacFilterSet` of the file */goform/WifiMacFilterSet* of the component *POST Parameter Handler*. The manipulation of the argument `index/GO` 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.

It is possible to read the advisory at github.com. The identification of this vulnerability is CVE-2026-3976. The exploitation is known to be easy. The attack may be initiated 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 vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-11517). Entries connected to this vulnerability are available at VDB-209506, VDB-214703, VDB-246453 and VDB-249059.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- W3

Version

- 1.0.0.3(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

03/11/2026		Advisory disclosed
03/11/2026	+0 days	VulDB entry created
03/17/2026	+6 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-3976 (🔒)
GCVE (CVE): GCVE-0-2026-3976
GCVE (VulDB): GCVE-100-350411
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/11/2026 03:07 PM
Updated: 03/17/2026 08:03 AM
Changes: 03/11/2026 03:07 PM (58), 03/11/2026 08:01 PM (2), 03/12/2026 06:26 AM (1), 03/17/2026 08:03 AM (32)
Complete: 🔍
Submitter: Svigo_o
Cache ID: 68:3FB:179

Submit

Accepted

- Submit #769179: Tenda W3 V1.0.0.3(2204) Buffer Overflow (by Svigo_o)

Duplicate

- [redacted]
- [redacted]
- [redacted]

Discussion

No comments yet. Languages: en.

Please log in to comment.