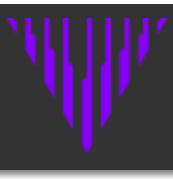

VDB-349771 · CVE-2026-3804 · EUVD-2026-10298

TENDA I3 1.0.0.6(2204) /GOFORM/WIFIMACFILTERSET FORMWIFIMACFILTERSET INDEX STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.21

Summary

A vulnerability identified as critical has been detected in Tenda i3 1.0.0.6(2204). This issue affects the function `formWifiMacFilterSet` of the file */goform/WifiMacFilterSet*. This manipulation of the argument *index* causes stack-based overflow. This vulnerability is handled as CVE-2026-3804. The attack can be initiated remotely. Additionally, an exploit exists.

Details

A vulnerability has been found in Tenda i3 1.0.0.6(2204) and classified as critical. Affected by this vulnerability is the function `formWifiMacFilterSet` of the file */goform/WifiMacFilterSet*. The manipulation of the argument `index` with an unknown input leads to a stack-based overflow vulnerability. The CWE definition for the vulnerability is 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). As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-3804. The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known.

It is possible to download the exploit 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-2026-10298). 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

- i3

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

03/08/2026		Advisory disclosed
03/08/2026	+0 days	VulDB entry created
03/09/2026	+1 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-3804 (🔒)
GCVE (CVE): GCVE-0-2026-3804
GCVE (VulDB): GCVE-100-349771
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/08/2026 01:44 PM
Updated: 03/09/2026 11:59 AM
Changes: 03/08/2026 01:44 PM (57), 03/09/2026 08:14 AM (31), 03/09/2026 11:59 AM (1)
Complete: 🔍
Submitter: Svigo
Cache ID: 172:8C1:179

Submit

Accepted

- Submit #768985: Tenda i3 V1.0.0.6(2204) Buffer Overflow (by Svigo)

Duplicate

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

Discussion

No comments yet. Languages: en.

Please log in to comment.