VDB-350530 · CVE-2026-4007 · EUVD-2026-11538

TENDA W3 1.0.0.3(2204) POST PARAMETER /GOFORM/WIFISSIDGET INDEX STACK-BASED OVERFLOW

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

Summary

A vulnerability described as critical has been identified in Tenda W3 1.0.0.3(2204). This issue affects some unknown processing of the file */goform/wifiSSIDget* of the component *POST Parameter Handler*. Executing a manipulation of the argument *index* can lead to stack-based overflow. This vulnerability is registered as CVE-2026-4007. It is possible to launch the attack remotely. Furthermore, an exploit is available.

Details

A vulnerability was found in Tenda W3 1.0.0.3(2204). It has been declared as critical. This vulnerability affects an unknown code block of the file */goform/wifiSSIDget* of the component *POST Parameter Handler*. 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.

The advisory is available at github.com. This vulnerability was named CVE-2026-4007. The exploitation appears to be easy. The attack can be initiated 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-2026-11538). Similar entries are available at VDB-206266, VDB-246459, VDB-262133 and VDB-262140.

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-2026-4007 (🔒)
GCVE (CVE): GCVE-0-2026-4007
GCVE (VulDB): GCVE-100-350530
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/11/2026 08:03 PM
Updated: 03/17/2026 10:08 AM
Changes: 03/11/2026 08:03 PM (57), 03/12/2026 12:18 PM (1), 03/17/2026 10:08 AM (32)
Complete: 🔍
Submitter: Svigo_o
Cache ID: 128:DC1:179

Submit

Accepted

- Submit #769181: Tenda W3 V1.0.0.3(2204) Buffer Overflow (by Svigo_o)

Duplicate

- [redacted]

Discussion

No comments yet. Languages: en.

Please log in to comment.