



VDB-350531 · CVE-2026-4008 · EUVD-2026-11540

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

CVSS Meta Temp Score ⓘ

8.4

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

0.45

## Summary

A vulnerability classified as **critical** has been found in **Tenda W3 1.0.0.3(2204)**. Impacted is an unknown function of the file */goform/wifiSSIDset* of the component *POST Parameter Handler*. The manipulation of the argument *index/GO* leads to stack-based overflow. This vulnerability is documented as **CVE-2026-4008**. The attack can be initiated remotely. Additionally, an exploit exists.

## Details

A vulnerability was found in **Tenda W3 1.0.0.3(2204)**. It has been rated as **critical**. This issue affects some unknown processing of the file */goform/wifiSSIDset* 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](https://github.com). The identification of this vulnerability is **CVE-2026-4008**. 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](https://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-2026-11540**). Entries connected to this vulnerability are available at [VDB-206269](#), [VDB-215148](#), [VDB-252257](#) and [VDB-252260](#).

## 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](https://tenda.com.cn)

**Advisory:** [github.com](https://github.com)

**Status:** Not defined

**CVE:** [CVE-2026-4008](#) (🔒)

**GCVE (CVE):** [GCVE-0-2026-4008](#)

**GCVE (VulDB):** [GCVE-100-350531](#)

**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 10:35 AM (1), 03/17/2026 10:08 AM (32)

**Complete:** 🔍

Submitter: [Svigo\\_o](#)

Cache ID: 40:2BC:179

## Submit

### Accepted

- [Submit #769182](#): Tenda W3 V1.0.0.3(2204) Buffer Overflow (by Svigo\_o)

### Duplicate

- [\[blurred link\]](#)
- [\[blurred link\]](#)
- [\[blurred link\]](#)

## Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)