VDB-350407 · CVE-2026-3972 · GCVE-100-350407

TENDA W3 1.0.0.3(2204) HTTP /GOFORM/SETCFM FORMSETCFM FUNCPARA1 STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.00

Summary

A vulnerability, which was classified as critical, has been found in Tenda W3 1.0.0.3(2204). This affects the function `formSetCfm` of the file */goform/setcfm* of the component *HTTP Handler*. This manipulation of the argument *funcpara1* causes stack-based overflow. This vulnerability is tracked as CVE-2026-3972. The attack is only possible within the local network. Moreover, an exploit is present.

Details

A vulnerability classified as critical was found in Tenda W3 1.0.0.3(2204). Affected by this vulnerability is the function `formSetCfm` of the file */goform/setcfm* of the component *HTTP Handler*. The manipulation of the argument `funcpara1` 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-2026-3972. The exploitation appears to be easy. The attack can only be done within the local network. The exploitation doesn't need any form of authentication. 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.

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: Partially

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-2026-3972 (🔒)
GCVE (CVE): GCVE-0-2026-3972
GCVE (VulDB): GCVE-100-350407
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 03/11/2026 03:06 PM
Updated: 03/17/2026 06:56 AM
Changes: 03/11/2026 03:06 PM (58), 03/17/2026 06:56 AM (31)
Complete: 🔍
Submitter: Svigo_o
Cache ID: 52:D14:179

Submit

Accepted

- Submit #769172: 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.