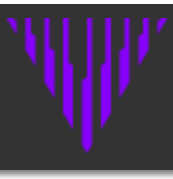

VDB-354187 · CVE-2026-5155 · GCVE-100-354187

TENDA CH22 1.0.0.1 PARAMETER /GOFORM/ADVSETWAN FROMADVSETWAN WANMODE STACK-BASED OVERFLOW

Summary

A vulnerability, which was classified as critical, has been found in Tenda CH22 1.0.0.1. This impacts the function `fromAdvSetWan` of the file */goform/AdvSetWan* of the component *Parameter Handler*. This manipulation of the argument *wanmode* causes stack-based overflow. This vulnerability is tracked as CVE-2026-5155. The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability classified as critical was found in Tenda CH22 1.0.0.1. Affected by this vulnerability is the function `fromAdvSetWan` of the file */goform/AdvSetWan* of the component *Parameter Handler*. The manipulation of the argument `wanmode` 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-2026-5155. 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 entries VDB-274768, VDB-274769, VDB-274789 and VDB-274796 are pretty similar.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- CH22

Version

- 1.0.0.1

License

- commercial

Website

- Vendor: https://www.tenda.com.cn/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 8.8
VulDB Meta Temp Score: 8.0

VulDB Base Score: 8.8
VulDB Temp Score: 8.0
VulDB Vector: 🔒
VulDB Reliability: 🔍

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: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

03/30/2026		Advisory disclosed
03/30/2026	+0 days	VulDB entry created
03/30/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5155 (🔒)
GCVE (CVE): GCVE-0-2026-5155
GCVE (VulDB): GCVE-100-354187
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/30/2026 03:38 PM
Changes: 03/30/2026 03:38 PM (58)
Complete: 🔍
Submitter: LtzHust2
Cache ID: 20:6E7:179

Submit

Accepted

- Submit #780207: Tenda CH22 V1.0.0.1 Stack-based Buffer Overflow (by LtzHust2)

Discussion

No comments yet. Languages: en.

Please log in to comment.