VDB-354186 · CVE-2026-5154 · GCVE-100-354186

TENDA CH22 1.0.0.1/1.IF PARAMETER /GOFORM/SETCFM FROMSETCFM FUNCNAME STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	3.00

Summary

A vulnerability classified as critical was found in Tenda CH22 1.0.0.1/1.If. This affects the function `fromSetCfm` of the file */goform/setcfm* of the component *Parameter Handler*. The manipulation of the argument *funcname* results in stack-based overflow. This vulnerability is identified as CVE-2026-5154. The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability classified as critical has been found in Tenda CH22 1.0.0.1/1.If. Affected is the function `fromSetCfm` of the file */goform/setcfm* of the component *Parameter Handler*. The manipulation of the argument `funcname` with an unknown input leads to a stack-based overflow vulnerability. CWE is classifying the issue as 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). This is going to have an impact on confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is traded as CVE-2026-5154. The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known.

The exploit is shared for download 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.

Entries connected to this vulnerability are available at VDB-260913, VDB-261143, VDB-275935 and VDB-307402.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- CH22

Version

- 1.0.0.1
- 1.If

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-2026-5154 (🔒)
GCVE (CVE): GCVE-0-2026-5154
GCVE (VulDB): GCVE-100-354186
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: 172:3B1:179

Submit

Accepted

- Submit #780206: Tenda CH22 V1.0.0.1 Stack-based Buffer Overflow (by LtzHust2)

Discussion

No comments yet. Languages: en.

Please log in to comment.