



VDB-354184 · CVE-2026-5152 · GCVE-100-354184

TENDA CH22 1.0.0.1 /GOFORM/CREATEFILENAME FORMCREATEFILENAME FILENAMEMIT STACK- BASED OVERFLOW

CVSS Meta Temp Score ⓘ

8.0

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

4.61

Summary

A vulnerability described as **critical** has been identified in **Tenda CH22 1.0.0.1**. The affected element is the function `formCreateFileName` of the file `/goform/createFileName`. Executing a manipulation of the argument `fileNameMit` can lead to stack-based overflow. The identification of this vulnerability is [CVE-2026-5152](#). The attack may be launched remotely. Furthermore, there is an exploit available.

Details

A vulnerability was found in **Tenda CH22 1.0.0.1**. It has been declared as critical. This vulnerability affects the function `formCreateFileName` of the file `/goform/createFileName`. The manipulation of the argument `fileNameMit` 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 shared for download at [github.com](#). This vulnerability was named [CVE-2026-5152](#). 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 entry [VDB-215138](#) is related to this item.

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

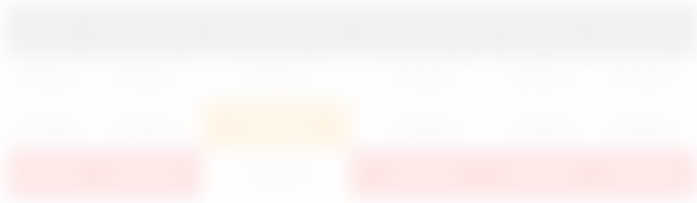
VulDB Base Score: 8.8

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-2026-5152](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5152](#)

GCVE (VulDB): [GCVE-100-354184](#)

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 (57)

Complete: 🔍

Submitter: [LtzHuster](#)

Cache ID: 74:AB4:179

Submit

Accepted

- [Submit #780203](#): Tenda CH22 V1.0.0.1 Stack-based Buffer Overflow (by LtzHuster)

Discussion

No comments yet. Languages: en.

Please log in to comment.