



VDB-355397 · CVE-2026-5605 · GCVE-100-355397

TENDA CH22 1.0.0.1 /GIFORM/WRLEXTRASET FORMWRLEXTRASET GO STACK-BASED OVERFLOW

CVSS Meta Temp Score

8.0

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

2.40

Summary

A vulnerability was found in [Tenda CH22 1.0.0.1](#). It has been rated as **critical**. This impacts the function `formWrIExtraSet` of the file `/goform/WrIExtraSet`. The manipulation of the argument `GO` leads to stack-based overflow. This vulnerability is uniquely identified as [CVE-2026-5605](#). The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability was found in [Tenda CH22 1.0.0.1](#) and classified as critical. This issue affects the function `formWrIExtraSet` of the file `/goform/WrIExtraSet`. The manipulation of the argument `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.

The advisory is shared at [github.com](#). The identification of this vulnerability is [CVE-2026-5605](#). 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](#). 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-349746](#), [VDB-352322](#) and [VDB-353969](#) 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

| | | |
|------------|---------|-------------------------|
| 04/05/2026 | | Advisory disclosed |
| 04/05/2026 | +0 days | VulDB entry created |
| 04/05/2026 | +0 days | VulDB entry last update |

Sources

Vendor: tenda.com.cn

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5605](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5605](#)

GCVE (VulDB): [GCVE-100-355397](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🔒

Entry

Created: 04/05/2026 04:05 PM

Changes: 04/05/2026 04:05 PM (57)

Complete: 🔍

Submitter: [LtzHuster](#)

Cache ID: 64:660:179

Submit

Accepted

- [Submit #785052](#): Tenda CH22 V1.0.0.1 Stack-based Buffer Overflow (by LtzHuster)

Discussion

No comments yet. Languages: en.

Please log in to comment.