



VDB-354185 · CVE-2026-5153 · GCVE-100-354185

TENDA CH22 1.0.0.1 /GOFORM/WRITEFACMAC FORMWRITEFACMAC MAC COMMAND INJECTION

CVSS Meta Temp Score 

5.7

Current Exploit Price (≈) 

\$0-\$5k

CTI Interest Score 

2.39

Summary

A vulnerability classified as **critical** has been found in **Tenda CH22 1.0.0.1**. The impacted element is the function `FormWriteFacMac` of the file `/goform/WriteFacMac`. The manipulation of the argument `mac` leads to command injection. This vulnerability is referenced as **CVE-2026-5153**. Remote exploitation of the attack is possible. Furthermore, an exploit is available.

Details

A vulnerability was found in **Tenda CH22 1.0.0.1**. It has been rated as **critical**. This issue affects the function `FormWriteFacMac` of the file `/goform/WriteFacMac`. The manipulation of the argument `mac` with an unknown input leads to a command injection vulnerability. Using CWE to declare the problem leads to **CWE-77**. The product constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is **CVE-2026-5153**. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique **T1202** for this issue.

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.

Similar entries are available at [VDB-257940](https://vuln.db.com/vuln/257940), [VDB-258151](https://vuln.db.com/vuln/258151), [VDB-258160](https://vuln.db.com/vuln/258160) and [VDB-258295](https://vuln.db.com/vuln/258295).

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: 6.3

VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3

VulDB Temp Score: 5.7

VulDB Vector: 

VulDB Reliability: 

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Command injection

CWE: [CWE-77](#) / [CWE-74](#) / [CWE-707](#)

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-2026-5153](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5153](#)

GCVE (VulDB): [GCVE-100-354185](#)

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: 20:EEA:179

Submit

Accepted

- [Submit #780204](#): Tenda CH22 V1.0.0.1 Command Injection (by LtzHuster)

Discussion

No comments yet. Languages: en.

Please log in to comment.