VDB-355396 · CVE-2026-5604 · GCVE-100-355396

TENDA CH22 1.0.0.1 PARAMETER CERTLOCALPRECREATE FORMCERTLOCALPRECREATE STANDARD STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	2.81

Summary

A vulnerability was found in Tenda CH22 1.0.0.1. It has been declared as critical. This affects the function `formCertLocalPrecreate` of the file */goform/CertLocalPrecreate* of the component *Parameter Handler*. Executing a manipulation of the argument *standard* can lead to stack-based overflow. This vulnerability is handled as CVE-2026-5604. The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability has been found in Tenda CH22 1.0.0.1 and classified as critical. This vulnerability affects the function `formCertLocalPrecreate` of the file */goform/CertLocalPrecreate* of the component *Parameter Handler*. The manipulation of the argument `standard` 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-2026-5604. 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.

Entries connected to this vulnerability are available at VDB-355410, VDB-355422, VDB-355423 and VDB-355424.

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

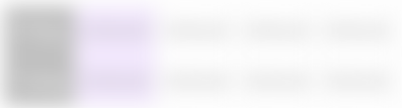
VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

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-2026-5604 (🔒)
GCVE (CVE): GCVE-0-2026-5604
GCVE (VulDB): GCVE-100-355396
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 04:04 PM
Changes: 04/05/2026 04:04 PM (58)
Complete: 🔍
Submitter: LtzHuster
Cache ID: 172:9C1:179

Submit

Accepted

- Submit #785032: Tenda CH22 V1.0.0.1 Stack-based Buffer Overflow (by LtzHuster)

Discussion

No comments yet. Languages: en.

Please log in to comment.