VDB-349706 · CVE-2026-3728 · EUVD-2026-10231

TENDA F453 1.0.0.3/1.IF /GOFORM/SETCFM FROMSETCFM FUNCNAME/FUNCPARA1 STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.11

Summary

A vulnerability classified as critical was found in Tenda F453 1.0.0.3/1.If. Impacted is the function `fromSetCfm` of the file */goform/setcfm*. Such manipulation of the argument *funcname/funcpara1* leads to stack-based overflow. This vulnerability is documented as CVE-2026-3728. The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability, which was classified as critical, has been found in Tenda F453 1.0.0.3/1.If. Affected by this issue is the function `fromSetCfm` of the file */goform/setcfm*. The manipulation of the argument `funcname/funcpara1` 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 available at github.com. This vulnerability is handled as CVE-2026-3728. The exploitation is known to be easy. The attack may be launched 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 vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-10231). 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

- F453

Version

- 1.0.0.3
- 1.If

License

- commercial

Website

- Vendor: https://www.tenda.com.cn/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 8.8
VulDB Meta Temp Score: 8.4

VulDB Base Score: 8.8
VulDB Temp Score: 8.0
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 8.8
CNA Vector: 🔒

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: 🔒

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

03/07/2026		Advisory disclosed
03/07/2026	+0 days	VulDB entry created
03/08/2026	+1 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-3728 (🔒)
GCVE (CVE): GCVE-0-2026-3728
GCVE (VulDB): GCVE-100-349706
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/07/2026 06:49 PM
Updated: 03/08/2026 06:58 PM

Changes: 03/07/2026 06:49 PM (57), 03/08/2026 03:07 PM (1), 03/08/2026 06:58 PM (31)

Complete: 🔍

Submitter: LtzHust

Cache ID: 135:374:179

Submit

Accepted

- Submit #766933: Tenda F453 v1.0.0.3 Stack-based Buffer Overflow (by LtzHust)

Discussion

No comments yet. Languages: en.

Please log in to comment.