VDB-349705 · CVE-2026-3727 · EUVD-2026-10230

TENDA F453 1.0.0.3 /GOFORM/QUICKINDEX SUB_3C6C0 MIT_LINKTYPE/PPPOEPASSWORD 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 has been found in Tenda F453 1.0.0.3. This issue affects the function `sub_3C6C0` of the file */goform/QuickIndex*. This manipulation of the argument *mit_linktype/PPPOEPassword* causes stack-based overflow. This vulnerability is registered as CVE-2026-3727. Remote exploitation of the attack is possible. Furthermore, an exploit is available.

Details

A vulnerability classified as critical was found in Tenda F453 1.0.0.3. Affected by this vulnerability is the function `sub_3C6C0` of the file */goform/QuickIndex*. The manipulation of the argument `mit_linktype/PPPOEPassword` 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 at github.com. This vulnerability is known as CVE-2026-3727. The exploitation appears to be easy. The attack can be launched 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 vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-10230).

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- F453

Version

- 1.0.0.3

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-2026-3727 (🔒)
GCVE (CVE): GCVE-0-2026-3727
GCVE (VulDB): GCVE-100-349705
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013

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: 20:586:179

Submit

Accepted

- Submit #766932: Tenda F453 v1.0.0.3 Stack-based Buffer Overflow (by LtzHust)

Discussion

No comments yet. Languages: en.

Please log in to comment.