



VDB-349581 · CVE-2026-3679 · EUVD-2026-10194

TENDA FH451 1.0.0.9 /GOFORM/QUICKINDEX FORMQUICKINDEX MIT_LINKTYPE/PPPOEPASSWORD STACK- BASED OVERFLOW

CVSS Meta Temp Score ⓘ

8.4

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

0.00

Summary

A vulnerability, which was classified as **critical**, has been found in **Tenda FH451 1.0.0.9**. Affected by this issue is the function `formQuickIndex` of the file `/goform/QuickIndex`. Performing a manipulation of the argument `mit_linktype/PPPOEPassword` results in stack-based overflow. This vulnerability is identified as **CVE-2026-3679**. The attack can be initiated remotely. Additionally, an exploit exists.

Details

A vulnerability, which was classified as **critical**, was found in **Tenda FH451 1.0.0.9**. This affects the function `formQuickIndex` of the file `/goform/QuickIndex`. The manipulation of the argument `mit_linktype/PPPOEPassword` with an unknown input leads to a stack-based overflow vulnerability. CWE is classifying the issue as **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). This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared at github.com. This vulnerability is uniquely identified as **CVE-2026-3679**. The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details and a public exploit are known.

The exploit is shared for download 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-2026-10194](https://euvd.com)).

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- FH451

Version

- 1.0.0.9

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

- 03/06/2026 | Advisory disclosed
- 03/06/2026 | +0 days | VulDB entry created
- 03/08/2026 | +2 days | VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-3679](https://cve.mitre.org/cve/2026/3679) (🔒)

GCVE (CVE): [GCVE-0-2026-3679](https://www.gdsc.com/gcve/0-2026-3679)

GCVE (VulDB): [GCVE-100-349581](https://www.gdsc.com/gcve/100-349581)

EUVD: 🔒

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

Entry

Created: 03/06/2026 10:27 PM

Updated: 03/08/2026 04:12 PM

Changes: 03/06/2026 10:27 PM (57), 03/08/2026 02:01 AM (1), 03/08/2026 04:12 PM (31)

Complete: 🔍

Submitter: LtzHuster

Cache ID: 4:ABE:179

Submit

Accepted

- [Submit #765331](#): Tenda FH451 V1.0.0.9 Stack-based Buffer Overflow (by LtzHuster)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)