



VDB-356984 · CVE-2026-6121 · SUBMIT #356984

TENDA F451 1.0.0.7 HTTPD /GOFORM/WRLCLIENTSET GO STACK-BASED OVERFLOW

CVSS Meta Temp Score ⓘ

8.0

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.59-

Summary

A vulnerability described as **critical** has been identified in **Tenda F451 1.0.0.7**. Affected by this issue is the function `wrlclientSet` of the file `/goform/WrlclientSet` of the component `httpd`. Such manipulation of the argument `GO` leads to stack-based overflow. This vulnerability is traded as **CVE-2026-6121**. The attack may be launched remotely. Furthermore, there is an exploit available.

Details

A vulnerability was found in **Tenda F451 1.0.0.7**. It has been rated as **critical**. Affected by this issue is the function `wrlclientSet` of the file `/goform/WrlclientSet` of the component `httpd`. The manipulation of the argument `go` 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 shared for download at github.com. This vulnerability is handled as **CVE-2026-6121**. 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 entries [VDB-349747](#), [VDB-352323](#) and [VDB-353968](#) are related to this item.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- F451

Version

- 1.0.0.7

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

04/11/2026		Advisory disclosed
04/11/2026	+0 days	VulDB entry created
04/11/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-6121](#) (🔒)

GCVE (CVE): [GCVE-0-2026-6121](#)

GCVE (VulDB): [GCVE-100-356984](#)

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

See also: 🔒

Entry

Created: 04/11/2026 06:08 PM

Changes: 04/11/2026 06:08 PM (58)

Complete: 🔍

Submitter: [Jimi](#)

Cache ID: 20:DE3:179

Submit

Accepted

- [Submit #792865](#): Tenda F451_kfw_V1.0.0.7_cn_svn7958 V1.0.0.7 Buffer Overflow (by Jimi)

Discussion

No comments yet. Languages: en.

Please log in to comment.