



VDB-356985 · CVE-2026-6122 · SUBMIT #356985

# TENDA F451 1.0.0.7 HTTPD /GOFORM/L7PROT FRML7PROTFORM PAGE STACK-BASED OVERFLOW

CVSS Meta Temp Score ⓘ

8.0

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

3.00-

## Summary

A vulnerability classified as **critical** has been found in **Tenda F451 1.0.0.7**. This affects the function `frmL7ProtForm` of the file `/goform/L7Prot` of the component `httpd`. Performing a manipulation of the argument `page` results in stack-based overflow. This vulnerability is known as **CVE-2026-6122**. Remote exploitation of the attack is possible. Furthermore, an exploit is available.

## Details

A vulnerability classified as **critical** has been found in **Tenda F451 1.0.0.7**. This affects the function `frmL7ProtForm` of the file `/goform/L7Prot` of the component `httpd`. The manipulation of the argument `page` 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](https://github.com). This vulnerability is uniquely identified as **CVE-2026-6122**. 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](https://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.

Similar entries are available at [VDB-234144](https://vuln.db.com/vuln/234144), [VDB-274785](https://vuln.db.com/vuln/274785), [VDB-316188](https://vuln.db.com/vuln/316188) and [VDB-316247](https://vuln.db.com/vuln/316247).

## 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](https://tenda.com.cn)

**Advisory:** [github.com](https://github.com)

**Status:** Not defined

**CVE:** [CVE-2026-6122](#) (🔒)

**GCVE (CVE):** [GCVE-0-2026-6122](#)

**GCVE (VulDB):** [GCVE-100-356985](#)

**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:** [Jxm666](#)

**Cache ID:** 128:640:179

## Submit

**Accepted**

- [Submit #792872](#): Tenda F451\_kfw\_V1.0.0.7\_cn\_svn7958 V1.0.0.7 Buffer Overflow (by Jxm666)

## Discussion

No comments yet. Languages: en.

Please log in to comment.