



VDB-349747 · CVE-2026-3769 · EUVD-2026-10272

# TENDA F453 1.0.0.3 /GOFORM/WRLCLIENTSET GO STACK-BASED OVERFLOW

## Summary

A vulnerability classified as **critical** has been found in **Tenda F453 1.0.0.3**. This affects the function `wrlclientSet` of the file `/goform/WrlclientSet`. This manipulation of the argument `GO` causes stack-based overflow. This vulnerability is tracked as **CVE-2026-3769**. The attack is possible to be carried out remotely. Moreover, an exploit is present.

## Details

A vulnerability was found in **Tenda F453 1.0.0.3**. It has been declared as critical. Affected by this vulnerability is the function `wrlclientSet` of the file `/goform/WrlclientSet`. The manipulation of the argument `go` 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.

It is possible to read the advisory at [github.com](https://github.com). This vulnerability is known as **CVE-2026-3769**. 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](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.

The vulnerability is also documented in the vulnerability database at EUVD (**EUVD-2026-10272**).

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

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

Status: Not defined

CVE: [CVE-2026-3769](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-3769](#)

GCVE (VulDB): [GCVE-100-349747](#)

EUVD: 🗝️

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

## Entry

Created: 03/07/2026 10:00 PM

Updated: 03/08/2026 11:33 PM

Changes: 03/07/2026 10:00 PM (57), 03/08/2026 11:14 PM (31), 03/08/2026 11:33 PM (1)

Complete: 🔍

Submitter: [LtzHust2](#)

Cache ID: 20:9C8:179

## Submit

### Accepted

- [Submit #768297](#): Tenda F453 v1.0.0.3 Stack-based Buffer Overflow (by LtzHust2)

## Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)