VDB-348265 · CVE-2026-3380 · EUVD-2026-9116

TENDA F453 1.0.0.3 /GOFORM/L7IM FRML7IMFORM PAGE BUFFER OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.10

Summary

A vulnerability, which was classified as critical, has been found in Tenda F453 1.0.0.3. Impacted is the function `frmL7ImForm` of the file */goform/L7Im*. This manipulation of the argument *page* causes buffer overflow. This vulnerability is registered as CVE-2026-3380. 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 `frmL7ImForm` of the file */goform/L7Im*. The manipulation of the argument `page` with an unknown input leads to a buffer overflow vulnerability. The CWE definition for the vulnerability is CWE-120. The product copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow. 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-2026-3380. 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 databases at CNNVD (CNNVD-202603-017) and EUVD (EUVD-2026-9116). Similar entries are available at VDB-215164, VDB-274770, VDB-274786 and VDB-307964.

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: Buffer overflow
CWE: CWE-120 / 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

02/28/2026		Advisory disclosed
02/28/2026	+0 days	VulDB entry created
03/02/2026	+2 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-3380 (🔒)
GCVE (CVE): GCVE-0-2026-3380
GCVE (VulDB): GCVE-100-348265
EUVD: 🔒
CNNVD: CNNVD-202603-017 - Tenda F453 安全漏洞

scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 02/28/2026 08:02 AM
Updated: 03/02/2026 05:13 PM
Changes: 02/28/2026 08:02 AM (57), 03/01/2026 07:27 PM (31), 03/01/2026 09:40 PM (1), 03/02/2026 03:56 PM (1), 03/02/2026 05:13 PM (6)
Complete: 🔍
Submitter: LtzHust2
Cache ID: 52:D60:179

Submit

Accepted

- Submit #759629: Tenda F453 v1.0.0.3 Buffer Access Using Size of Source Buffer (by LtzHust2)

Discussion

No comments yet. Languages: en.

Please log in to comment.