VDB-357000 · CVE-2026-6136 · SUBMIT #357000

TENDA F451 1.0.0.7_CN_SVN7958 /GOFORM/L7IM FRML7IMFORM PAGE STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	2.88-

Summary

A vulnerability classified as critical was found in Tenda F451 1.0.0.7_cn_svn7958. The affected element is the function `frmL7ImForm` of the file */goform/L7Im*. The manipulation of the argument *page* results in stack-based overflow. This vulnerability is known as CVE-2026-6136. It is possible to launch the attack remotely. Furthermore, an exploit is available.

Details

A vulnerability was found in Tenda F451 1.0.0.7_cn_svn7958. It has been classified as critical. Affected is the function `frmL7ImForm` of the file */goform/L7Im*. 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 for download at github.com. This vulnerability is traded as CVE-2026-6136. The exploitability is told to be easy. It is possible to launch 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-2026-21756).

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- F451

Version

- 1.0.0.7_cn_svn7958

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

04/12/2026		Advisory disclosed
04/12/2026	+0 days	VulDB entry created
04/13/2026	+1 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-6136 (🔒)
GCVE (CVE): GCVE-0-2026-6136
GCVE (VulDB): GCVE-100-357000
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/12/2026 09:28 AM
Updated: 04/13/2026 03:44 AM
Changes: 04/12/2026 09:28 AM (57), 04/13/2026 03:44 AM (1)
Complete: 🔍
Submitter: Jxm666
Cache ID: 57:1C0:179

Submit

Accepted

- Submit #792880: 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.

© 1997-2026 vuldb.com · cc by-nc-sa

v20.3.3