VDB-348261 · CVE-2026-3376 · EUVD-2026-9112

TENDA F453 1.0.0.3 /GOFORM/SAFEMACFILTER FROMSAFEMACFILTER PAGE BUFFER OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.29

Summary

A vulnerability marked as critical has been reported in Tenda F453 1.0.0.3. Affected by this issue is the function `fromSafeMacFilter` of the file */goform/SafeMacFilter*. Performing a manipulation of the argument *page* results in buffer overflow. This vulnerability is identified as CVE-2026-3376. The attack can be initiated remotely. Additionally, an exploit exists.

Details

A vulnerability was found in Tenda F453 1.0.0.3. It has been classified as critical. This affects the function `fromSafeMacFilter` of the file */goform/SafeMacFilter*. The manipulation of the argument `page` with an unknown input leads to a buffer overflow vulnerability. CWE is classifying the issue as 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. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared at github.com. This vulnerability is uniquely identified as CVE-2026-3376. 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. 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-2026-9112). Entries connected to this vulnerability are available at VDB-215160, VDB-234148, VDB-312579 and VDB-329904.

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-2026-3376 (🔒)
GCVE (CVE): GCVE-0-2026-3376
GCVE (VulDB): GCVE-100-348261
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 02/28/2026 08:00 AM
Updated: 03/02/2026 03:56 PM
Changes: 02/28/2026 08:00 AM (57), 03/01/2026 05:57 AM (1), 03/01/2026 07:27 PM (31), 03/02/2026 03:56 PM (1)
Complete: 🔍
Submitter: LtzHust2
Cache ID: 172:7C5:179

Submit

Accepted

- Submit #759623: Tenda F453 v1.0.0.3 Buffer Access Using Size of Source Buffer (by LtzHust2)

Duplicate

- [redacted]

Discussion

No comments yet. Languages: en.

Please log in to comment.