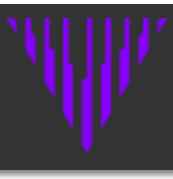

VDB-356544 · CVE-2026-5990 · GCVE-100-356544

TENDA F451 1.0.0.7 /GOFORM/SAFEEMAILFILTER FROMSAFEEMAILFILTER PAGE STACK-BASED OVERFLOW

CVSS Meta Temp Score

8.0

Current Exploit Price (≈)

$0-$5k

CTI Interest Score

1.50

Summary

A vulnerability was found in Tenda F451 1.0.0.7. It has been declared as critical. Affected by this issue is the function `fromSafeEmailFilter` of the file */goform/SafeEmailFilter*. The manipulation of the argument *page* results in stack-based overflow. This vulnerability is cataloged as CVE-2026-5990. The attack may be launched remotely. Furthermore, there is an exploit available.

Details

A vulnerability classified as critical has been found in Tenda F451 1.0.0.7. Affected is the function `fromSafeEmailFilter` of the file */goform/SafeEmailFilter*. 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-2026-5990. 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.

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

04/09/2026		Advisory disclosed
04/09/2026	+0 days	VulDB entry created
04/09/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5990 (🔒)
GCVE (CVE): GCVE-0-2026-5990
GCVE (VulDB): GCVE-100-356544
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/09/2026 02:42 PM
Changes: 04/09/2026 02:42 PM (57)
Complete: 🔍
Submitter: Jimi
Cache ID: 52:551:179

Submit

Accepted

- Submit #792861: Tenda F451_kfw_V1.0.0.7_cn_svn7958 V1.0.0.7 Buffer Overflow (by Jimi)

Discussion

No comments yet. Languages: en.

Please log in to comment.