VDB-349777 · CVE-2026-3811 · EUVD-2026-10312

TENDA FH1202 1.2.0.14(408) /GOFORM/P2PLISTFILTER FROMP2PLISTFILTER PAGE STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.33

Summary

A vulnerability, which was classified as critical, has been found in Tenda FH1202 1.2.0.14(408). Affected is the function `fromP2pListFilter` of the file */goform/P2pListFilter*. This manipulation of the argument *page* causes stack-based overflow. This vulnerability is tracked as CVE-2026-3811. The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability classified as critical was found in Tenda FH1202 1.2.0.14(408). Affected by this vulnerability is the function `fromP2pListFilter` of the file */goform/P2pListFilter*. The manipulation of the argument `page` 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.

The advisory is shared at github.com. This vulnerability is known as CVE-2026-3811. 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 vulnerability database at EUVD (EUVD-2026-10312). The entries VDB-215155, VDB-234147, VDB-274767 and VDB-274790 are pretty similar.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- FH1202

Version

- 1.2.0.14(408)

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

03/08/2026		Advisory disclosed
03/08/2026	+0 days	VulDB entry created
03/09/2026	+1 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-3811 (🔒)
GCVE (CVE): GCVE-0-2026-3811
GCVE (VulDB): GCVE-100-349777
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/08/2026 05:28 PM
Updated: 03/09/2026 11:44 AM
Changes: 03/08/2026 05:28 PM (57), 03/09/2026 11:00 AM (31), 03/09/2026 11:44 AM (2)
Complete: 🔍

Submitter: m202572177
Cache ID: 172:960:179

Submit

Accepted

- Submit #769041: Tenda FH1202 V1.2.0.14(408) Buffer Overflow (by m202572177)

Discussion

No comments yet. Languages: en.

Please log in to comment.