VDB-348293 · CVE-2026-3398 · EUVD-2026-9131

TENDA F453 1.0.0.3 HTTPD /GOFORM/ADVSETWAN FROMADVSETWAN WANMODE/PPPOEPASSWORD 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. Affected by this vulnerability is the function `fromAdvSetWan` of the file */goform/AdvSetWan* of the component *httpd*. The manipulation of the argument *wanmode/PPPOEPassword* leads to buffer overflow. This vulnerability is listed as CVE-2026-3398. The attack may be initiated remotely. In addition, an exploit is available.

Details

A vulnerability, which was classified as critical, has been found in Tenda F453 1.0.0.3. This issue affects the function `fromAdvSetWan` of the file */goform/AdvSetWan* of the component *httpd*. The manipulation of the argument `wanmode/PPPOEPassword` with an unknown input leads to a buffer overflow vulnerability. Using CWE to declare the problem leads to 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. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-3398. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known.

The exploit is available 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-2026-9131). See VDB-274768, VDB-274769, VDB-274789 and VDB-274796 for similar entries.

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

03/01/2026		Advisory disclosed
03/01/2026	+0 days	VulDB entry created
03/03/2026	+2 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-3398 (🔒)
GCVE (CVE): GCVE-0-2026-3398
GCVE (VulDB): GCVE-100-348293
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/01/2026 07:39 AM
Updated: 03/03/2026 03:23 PM
Changes: 03/01/2026 07:39 AM (58), 03/02/2026 12:05 AM (31), 03/02/2026 03:19 AM (1), 03/03/2026 03:23 PM (1)
Complete: 🔍
Submitter: LtzHust2
Cache ID: 20:1F8:179

Submit

Accepted

- Submit #759630: 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.