VDB-347997 · CVE-2026-3273 · GCVE-100-347997

TENDA F453 1.0.0.3 HTTPD /GOFORM/ADVSETWRLSAFESET FORMWRLSAFESET MIT_SSID_INDEX BUFFER OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	0.00

Summary

A vulnerability classified as critical has been found in Tenda F453 1.0.0.3. Affected by this issue is the function `formWrlsafeset` of the file */goform/AdvSetWrlsafeset* of the component *httpd*. Performing a manipulation of the argument *mit_ssid_index* results in buffer overflow. This vulnerability is reported as CVE-2026-3273. The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability, which was classified as critical, was found in Tenda F453 1.0.0.3. This affects the function `formWrlsafeset` of the file */goform/AdvSetWrlsafeset* of the component *httpd*. The manipulation of the argument `mit_ssid_index` 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-2026-3273. 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 entries VDB-215140, VDB-236349, VDB-275685 and VDB-302041 are pretty similar.

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: 🔍

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: 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

02/26/2026		Advisory disclosed
02/26/2026	+0 days	VulDB entry created
02/26/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-3273 (🔒)
GCVE (CVE): GCVE-0-2026-3273
GCVE (VulDB): GCVE-100-347997
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 02/26/2026 04:21 PM
Changes: 02/26/2026 04:21 PM (58)
Complete: 🔍
Submitter: LtzHust
Cache ID: 172:CE2:179

Submit

Accepted

- Submit #759606: Tenda F453 v1.0.0.3 Buffer Access Using Size of Source Buffer (by LtzHust)

Discussion

No comments yet. Languages: en.

Please log in to comment.