



VDB-349773 · CVE-2026-3807 · EUVD-2026-10300

TENDA FH1202 1.2.0.14(408) /GIFORM/ADVSETWRLSAFESET FORMWRLSAFESET MIT_SSID/MIT_SSID_INDEX STACK-BASED OVERFLOW

CVSS Meta Temp Score ⓘ

8.4

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

0.11

Summary

A vulnerability marked as **critical** has been reported in [Tenda FH1202 1.2.0.14\(408\)](#). The affected element is the function `formWrIsafeset` of the file `/goform/AdvSetWrIsafeset`. Performing a manipulation of the argument `mit_ssid/mit_ssid_index` results in stack-based overflow. This vulnerability was named [CVE-2026-3807](#). The attack may be initiated remotely. In addition, an exploit is available.

Details

A vulnerability was found in [Tenda FH1202 1.2.0.14\(408\)](#). It has been classified as critical. This affects the function `formWrIsafeset` of the file `/goform/AdvSetWrIsafeset`. The manipulation of the argument `mit_ssid/mit_ssid_index` 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 at [github.com](#). This vulnerability is uniquely identified as [CVE-2026-3807](#). 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-2026-10300](#)). See [VDB-215140](#), [VDB-236349](#), [VDB-275685](#) and [VDB-302041](#) for similar entries.

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-2026-3807](https://cve.mitre.org/cve/2026/3807) (🔒)

GCVE (CVE): [GCVE-0-2026-3807](https://www.gdsc.com.cn/gcve/0-2026-3807)

GCVE (VulDB): [GCVE-100-349773](https://www.gdsc.com.cn/gcve/100-349773)

EUVD: 🔒

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🔒

Entry

Created: 03/08/2026 05:28 PM

Updated: 03/09/2026 11:59 AM

Changes: 03/08/2026 05:28 PM (57), 03/09/2026 11:00 AM (31), 03/09/2026 11:59 AM (1)

Complete: 🔍

Submitter: Fan95

Cache ID: 52:245:179

Submit

Accepted

- [Submit #769019](#): Tenda FH1202 V1.2.0.14(408) Buffer Overflow (by Fan95)

Duplicate

- [\[Redacted\]](#)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)