VDB-353969 · CVE-2026-5046 · GCVE-100-353969

TENDA FH1201 1.2.0.14(408) PARAMETER /GOFORM/WRLEXTRASET FORMWRLEXTRASET GO STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	0.34

Summary

A vulnerability was found in Tenda FH1201 1.2.0.14(408). It has been rated as critical. Affected by this vulnerability is the function `formWrlExtraSet` of the file */goform/WrlExtraSet* of the component *Parameter Handler*. The manipulation of the argument *GO* leads to stack-based overflow. This vulnerability is traded as CVE-2026-5046. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability was found in Tenda FH1201 1.2.0.14(408). It has been rated as critical. This issue affects the function `formWrlExtraSet` of the file */goform/WrlExtraSet* of the component *Parameter Handler*. The manipulation of the argument `GO` with an unknown input leads to a stack-based overflow vulnerability. Using CWE to declare the problem leads to 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). Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-5046. 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 entries VDB-349746 and VDB-352322 are related to this item.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- FH1201

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: 🔍

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

03/27/2026		Advisory disclosed
03/27/2026	+0 days	VulDB entry created
03/27/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5046 (🔒)
GCVE (CVE): GCVE-0-2026-5046
GCVE (VulDB): GCVE-100-353969
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/27/2026 05:43 PM
Changes: 03/27/2026 05:43 PM (58)
Complete: 🔍
Submitter: LtzHuster2
Cache ID: 64:177:179

Submit

Accepted

- Submit #779127: Tenda FH1201 1.2.0.14(408) Stack-based Buffer Overflow (by LtzHuster2)

Discussion

No comments yet. Languages: en.

Please log in to comment.