VDB-348295 · CVE-2026-3400 · EUVD-2026-9133

TENDA AC15 UP TO 15.13.07.13 TEXTEDITINGCONVERSION WPAPSK_CRYPTO2_4G STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.9	$0-$5k	0.22

Summary

A vulnerability has been found in Tenda AC15 up to 15.13.07.13 and classified as critical. This affects an unknown part of the file */goform/TextEditingConversion*. This manipulation of the argument *wpapsk_crypto2_4g* causes stack-based overflow. This vulnerability is registered as CVE-2026-3400. Remote exploitation of the attack is possible. Furthermore, an exploit is available.

Details

A vulnerability has been found in Tenda AC15 up to 15.13.07.13 and classified as critical. Affected by this vulnerability is an unknown part of the file */goform/TextEditingConversion*. The manipulation of the argument `wpapsk_crypto2_4g` 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.

It is possible to read the advisory at yuque.com. This vulnerability is known as CVE-2026-3400. 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 yuque.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 databases at CNNVD (CNNVD-202603-021) and EUVD (EUVD-2026-9133). Similar entries are available at VDB-237180, VDB-250702 and VDB-330913.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- AC15

Version

- 15.13.07.0
- 15.13.07.1
- 15.13.07.2
- 15.13.07.3
- 15.13.07.4
- 15.13.07.5
- 15.13.07.6
- 15.13.07.7
- 15.13.07.8
- 15.13.07.9
- 15.13.07.10
- 15.13.07.11
- 15.13.07.12
- 15.13.07.13

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

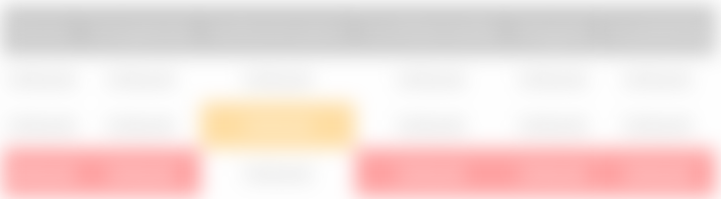
VulDB Meta Base Score: 9.1
VulDB Meta Temp Score: 8.9

VulDB Base Score: 8.8
VulDB Temp Score: 8.0
VulDB Vector: 🔒
VulDB Reliability: 🔍

NVD Base Score: 9.8
NVD Vector: 🔒

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

03/01/2026		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: yuque.com
Status: Not defined

CVE: CVE-2026-3400 (🔒)
GCVE (CVE): GCVE-0-2026-3400
GCVE (VulDB): GCVE-100-348295
EUVD: 🔒
CNNVD: CNNVD-202603-021 - Tenda AC15 安全漏洞

scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/01/2026 07:41 AM
Updated: 03/03/2026 11:29 PM
Changes: 03/01/2026 07:41 AM (56), 03/02/2026 02:17 AM (31), 03/02/2026 03:19 AM (1), 03/02/2026 05:13 PM (6), 03/03/2026 03:23 PM (1), 03/03/2026 11:29 PM (11)
Complete: 🔍
Submitter: Xuhsy
Cache ID: 172:397:179

Submit

Accepted

- Submit #760109: Tenda A15 V15.13.07.13 Stack-based Buffer Overflow (by Xuhsy)

Discussion

No comments yet. Languages: en.

Please log in to comment.