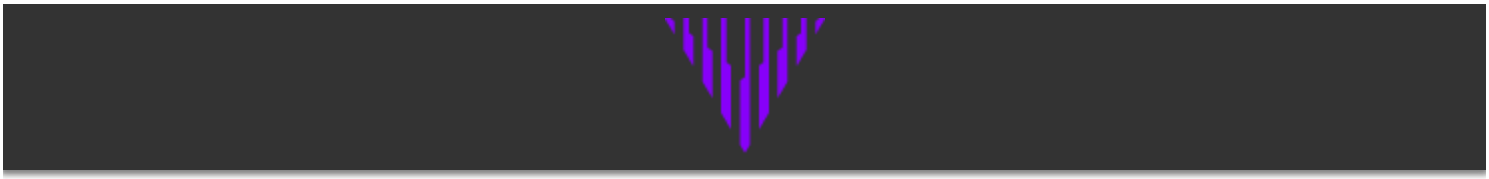

VDB-351212 · CVE-2026-4254 · EUVD-2026-12488

TENDA AC8 UP TO 16.03.50.11 HTTP ENDPOINT /GOFORM/SYSTOOLCHANGEPWD DOSYSTEMCMD LOCAL_2C STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
9.4	$0-$5k	0.11

Summary

A vulnerability categorized as critical has been discovered in Tenda AC8 up to 16.03.50.11. This issue affects the function `doSystemCmd` of the file */goform/SysToolChangePwd* of the component *HTTP Endpoint*. Such manipulation of the argument *local_2c* leads to stack-based overflow. This vulnerability is uniquely identified as CVE-2026-4254. The attack can be launched remotely. Moreover, an exploit is present.

Details

A vulnerability was found in Tenda AC8 up to 16.03.50.11 and classified as critical. Affected by this issue is the function `doSystemCmd` of the file */goform/SysToolChangePwd* of the component *HTTP Endpoint*. The manipulation of the argument `local_2c` 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 for download at github.com. This vulnerability is handled as CVE-2026-4254. The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. 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-2026-12488). The entries VDB-123487, VDB-126133, VDB-217124 and VDB-258708 are pretty similar.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- AC8

Version

- 16.03.50.0
- 16.03.50.1
- 16.03.50.2
- 16.03.50.3
- 16.03.50.4
- 16.03.50.5
- 16.03.50.6
- 16.03.50.7
- 16.03.50.8
- 16.03.50.9
- 16.03.50.10
- 16.03.50.11

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: 9.8
VulDB Meta Temp Score: 9.4

VulDB Base Score: 9.8
VulDB Temp Score: 8.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 9.8
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

03/16/2026		Advisory disclosed
03/16/2026	+0 days	VulDB entry created
03/21/2026	+5 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com

Status: Not defined

CVE: CVE-2026-4254 (🔒)
GCVE (CVE): GCVE-0-2026-4254
GCVE (VulDB): GCVE-100-351212
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/16/2026 07:21 AM
Updated: 03/21/2026 02:09 PM
Changes: 03/16/2026 07:21 AM (58), 03/17/2026 08:39 AM (1), 03/21/2026 02:09 PM (32)
Complete: 🔍
Submitter: DigitalAndrew
Cache ID: 104:B58:179

Submit

Accepted

- Submit #771773: Tenda AC8 V5 V16.03.50.11 Buffer Overflow (by DigitalAndrew)

Discussion

No comments yet. Languages: en.

Please log in to comment.