VDB-352019 · CVE-2026-4493 · EUVD-2026-13754

TENDA A18 PRO 02.03.02.28 MAC FILTERING CONFIGURATION ENDPOINT /GOFORM/SETMACFILTERCFG SUB_423B50 DEVICELIST STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.23

Summary

A vulnerability has been found in Tenda A18 Pro 02.03.02.28 and classified as critical. This affects the function `sub_423B50` of the file */goform/setMacFilterCfg* of the component *MAC Filtering Configuration Endpoint*. The manipulation of the argument *deviceList* leads to stack-based overflow. This vulnerability is traded as CVE-2026-4493. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability, which was classified as critical, has been found in Tenda A18 Pro 02.03.02.28. This issue affects the function `sub_423B50` of the file */goform/setMacFilterCfg* of the component *MAC Filtering Configuration Endpoint*. The manipulation of the argument `deviceList` 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.

It is possible to read the advisory at github.com. The identification of this vulnerability is CVE-2026-4493. 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 vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-13754).

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- A18 Pro

Version

- 02.03.02.28

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

03/20/2026		Advisory disclosed
03/20/2026	+0 days	VulDB entry created
03/26/2026	+6 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-4493 (🔒)
GCVE (CVE): GCVE-0-2026-4493
GCVE (VulDB): GCVE-100-352019
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 03/20/2026 09:38 AM
Updated: 03/26/2026 11:31 PM
Changes: 03/20/2026 09:38 AM (58), 03/21/2026 05:18 AM (1), 03/26/2026 11:31 PM (32)
Complete: 🔍

Submitter: lilukun
Cache ID: 20:F6A:179

Submit

Accepted

- Submit #773727: Tenda A18pro V02.03.02.28 Stack-based Buffer Overflow (by lilukun)

Discussion

No comments yet. Languages: en.

Please log in to comment.