VDB-352017 · CVE-2026-4491 · EUVD-2026-13738

TENDA A18 PRO 02.03.02.28 /GOFORM/SETIPMACBIND FROMSETIPMACBIND LIST STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.4	$0-$5k	0.22

Summary

A vulnerability, which was classified as critical, has been found in Tenda A18 Pro 02.03.02.28. The affected element is the function `fromSetIpMacBind` of the file */goform/SetIpMacBind*. Performing a manipulation of the argument *list* results in stack-based overflow. This vulnerability is reported as CVE-2026-4491. The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability classified as critical has been found in Tenda A18 Pro 02.03.02.28. This affects the function `fromSetIpMacBind` of the file */goform/SetIpMacBind*. The manipulation of the argument `list` 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-2026-4491. 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-2026-13738). The entries VDB-271074, VDB-298121, VDB-320357 and VDB-320930 are pretty similar.

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-2026-4491 (🔒)
GCVE (CVE): GCVE-0-2026-4491
GCVE (VulDB): GCVE-100-352017
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/20/2026 09:38 AM
Updated: 03/26/2026 10:24 PM
Changes: 03/20/2026 09:38 AM (57), 03/20/2026 08:05 PM (1), 03/26/2026 10:24 PM (32)

Complete: 🔍

Submitter: lilukun

Cache ID: 52:0EC:179

Submit

Accepted

- Submit #773671: Tenda A18pro V02.03.02.28 Stack-based Buffer Overflow (by lilukun)

Discussion

No comments yet. Languages: en.

Please log in to comment.