VDB-355313 · CVE-2026-5549 · GCVE-100-355313

TENDA AC10 16.03.10.10_MULTI_TDE01 RSA 2048-BIT PRIVATE KEY PRIVKEYSRV.PEM HARD-CODED KEY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.7	$0-$5k	1.93-

Summary

A vulnerability was found in Tenda AC10 16.03.10.10_multi_TDE01. It has been rated as problematic. This affects an unknown part of the file */webroot_ro/pem/privkeySrv.pem* of the component *RSA 2048-bit Private Key Handler*. The manipulation leads to hard-coded key. This vulnerability is listed as CVE-2026-5549. The attack may be initiated remotely. In addition, an exploit is available. It is recommended to apply restrictive firewalling.

Details

A vulnerability, which was classified as problematic, has been found in Tenda AC10 16.03.10.10_multi_TDE01. This issue affects an unknown function of the file */webroot_ro/pem/privkeySrv.pem* of the component *RSA 2048-bit Private Key Handler*. The manipulation with an unknown input leads to a hard-coded key vulnerability. Using CWE to declare the problem leads to CWE-321. The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered. Impacted is confidentiality.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-5549. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1600.001 for this issue.

The exploit is available at github.com. It is declared as proof-of-concept.

Addressing this vulnerability is possible by firewalling .

See VDB-321809, VDB-321810, VDB-321820 and VDB-321821 for similar entries.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- AC10

Version

- 16.03.10.10_multi_TDE01

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: 5.3
VulDB Meta Temp Score: 4.7

VulDB Base Score: 5.3
VulDB Temp Score: 4.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Hard-coded key
CWE: CWE-321 / CWE-320
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: Firewall
Status: 🔍

0-Day Time: 🔒

Timeline

04/04/2026		Advisory disclosed
04/04/2026	+0 days	VulDB entry created
04/04/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5549 (🔒)
GCVE (CVE): GCVE-0-2026-5549
GCVE (VulDB): GCVE-100-355313
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 03:33 PM
Changes: 04/04/2026 03:33 PM (57)
Complete: 🔍
Submitter: CoreNode
Cache ID: 20:8E3:179

Submit

Accepted

- Submit #782298: Tenda AC10 V4 US_AC10V4.0si_V16.03.10.10_multi_TDE01 Cryptographic Issues (by CoreNode)

Discussion

No comments yet. Languages: en.

Please log in to comment.