VDB-355280 · CVE-2026-5527 · GCVE-100-355280

TENDA 4G03 PRO 1.0/1.0RE/01.BIN/04.03.01.53 ECDSA P-256 PRIVATE KEY /ETC/WWW/PEM/SERVER.KEY HARD-CODED KEY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.7	$0-$5k	2.16

Summary

A vulnerability, which was classified as problematic, was found in Tenda 4G03 Pro 1.0/1.0re/01.bin/04.03.01.53. This affects an unknown part of the file */etc/www/pem/server.key* of the component *ECDSA P-256 Private Key Handler*. Such manipulation leads to hard-coded key. This vulnerability is referenced as CVE-2026-5527. It is possible to launch the attack remotely. Furthermore, an exploit is available. Restrictive firewalling should be applied.

Details

A vulnerability was found in Tenda 4G03 Pro 1.0/1.0re/01.bin/04.03.01.53 and classified as problematic. Affected by this issue is some unknown functionality of the file */etc/www/pem/server.key* of the component *ECDSA P-256 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.

This vulnerability is handled as CVE-2026-5527. 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 exploit are known. The MITRE ATT&CK project declares the attack technique as T1600.001.

It is declared as proof-of-concept.

Addressing this vulnerability is possible by firewalling .

Similar entries are available at VDB-333199, VDB-333200 and VDB-355279.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- 4G03 Pro

Version

- 1.0
- 1.0re
- 01.bin
- 04.03.01.53

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: 🔒
Status: Proof-of-Concept
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

Status: Not defined

CVE: CVE-2026-5527 (🔒)
GCVE (CVE): GCVE-0-2026-5527
GCVE (VulDB): GCVE-100-355280
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 08:25 AM
Changes: 04/04/2026 08:25 AM (54)
Complete: 🔍
Submitter: CoreNode
Cache ID: 52:A14:179

Submit

Accepted

- Submit #782053: Tenda 4G03 Pro V1.0 V04.03.01.53 Cryptographic Issues (by CoreNode)

Discussion

No comments yet. Languages: en.

Please log in to comment.