VDB-355279 · CVE-2026-5526 · GCVE-100-355279

TENDA 4G03 PRO UP TO 1.0/1.1/04.03.01.53/192.168.0.1 /BIN/HTTPD ACCESS CONTROL

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

6.4 | $0-$5k | 1.41

Summary

A vulnerability, which was classified as critical, has been found in Tenda 4G03 Pro up to 1.0/1.1/04.03.01.53/192.168.0.1. Affected by this issue is some unknown functionality of the file */bin/httpd*. This manipulation causes access control. The identification of this vulnerability is CVE-2026-5526. It is possible to initiate the attack remotely. Furthermore, there is an exploit available. It is advisable to implement restrictive firewalling.

Details

A vulnerability has been found in Tenda 4G03 Pro up to 1.0/1.1/04.03.01.53/192.168.0.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file */bin/httpd*. The manipulation with an unknown input leads to a access control vulnerability. The CWE definition for the vulnerability is CWE-284. The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor. As an impact it is known to affect confidentiality, integrity, and availability.

This vulnerability is known as CVE-2026-5526. The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1068 according to MITRE ATT&CK.

It is declared as proof-of-concept.

Proper firewalling of is able to address this issue.

The entries VDB-304982, VDB-305656, VDB-305657 and VDB-305726 are related to this item.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- 4G03 Pro

Version

- 1.0
- 1.1
- 04.03.01.0
- 04.03.01.1
- 04.03.01.2
- 04.03.01.3
- 04.03.01.4
- 04.03.01.5
- 04.03.01.6
- 04.03.01.7
- 04.03.01.8
- 04.03.01.9
- 04.03.01.10
- 04.03.01.11
- 04.03.01.12

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: 7.3
VulDB Meta Temp Score: 6.4

VulDB Base Score: 7.3
VulDB Temp Score: 6.4
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Access control
CWE: CWE-284 / CWE-266
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public

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-2026-5526 (🔒)
GCVE (CVE): GCVE-0-2026-5526
GCVE (VulDB): GCVE-100-355279
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: 20:B21:179

Submit

Accepted

- Submit #782052: Tenda Tenda 4G03 Pro V1.0 V04.03.01.53 Authentication Bypass Issues (by CoreNode)

Discussion

No comments yet. Languages: en.

Please log in to comment.