



VDB-355311 · CVE-2026-5547 · GCVE-100-355311

TENDA AC10 16.03.10.10_MULTI_TDE01 /BIN/HTTPD FORMADDMACFILTERRULE OS COMMAND INJECTION

CVSS Meta Temp Score 

6.1

Current Exploit Price (≈) 

\$0-\$5k

CTI Interest Score 

1.69-

Summary

A vulnerability was found in [Tenda AC10 16.03.10.10_multi_TDE01](#). It has been classified as **critical**. Affected by this vulnerability is the function `formAddMacfilterRule` of the file `/bin/httpd`. Performing a manipulation results in `os` command injection. This vulnerability is identified as [CVE-2026-5547](#). The attack can be initiated remotely. There is not any exploit available. Multiple endpoints might be affected.

Details

A vulnerability classified as **critical** has been found in [Tenda AC10 16.03.10.10_multi_TDE01](#). This affects the function `formAddMacfilterRule` of the file `/bin/httpd`. The manipulation with an unknown input leads to a `os` command injection vulnerability. CWE is classifying the issue as [CWE-78](#). The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at [github.com](#). This vulnerability is uniquely identified as [CVE-2026-5547](#). The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details of the vulnerability are known, but there is no available exploit. The pricing for an exploit might be around USD \$0-\$5k at the moment ([estimation calculated on 04/04/2026](#)). The attack technique deployed by this issue is [T1202](#) according to MITRE ATT&CK.

Multiple endpoints might be affected.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Entries connected to this vulnerability are available at [VDB-304982](#), [VDB-305656](#), [VDB-305657](#) and [VDB-305726](#).

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: 6.3

VulDB Meta Temp Score: 6.1

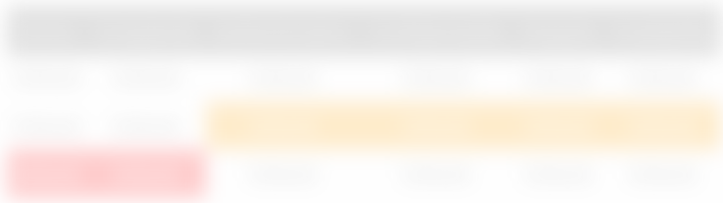
VulDB Base Score: 6.3

VulDB Temp Score: 6.1

VulDB Vector: 

VulDB Reliability: 

CVSSv2



VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Os command injection

CWE: [CWE-78](#) / [CWE-77](#) / [CWE-74](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

Local: No

Remote: Yes

Availability: 🔒

Status: Not defined

Price Prediction: 🔍

Current Price Estimation: 🔒



Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known

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-2026-5547](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5547](#)

GCVE (VulDB): [GCVE-100-355311](#)

See also: 🗝️

Entry

Created: 04/04/2026 03:33 PM

Changes: 04/04/2026 03:33 PM (54)

Complete: 🔍

Submitter: [CoreNode](#)

Cache ID: 64:BF3:179

Submit

Accepted

- [Submit #782296](#): Tenda AC10 V4 US_AC10V4.0si_V16.03.10.10_multi_TDE01 OS Command Injection (by CoreNode)

Discussion

No comments yet. Languages: en.

Please log in to comment.