VDB-351211 · CVE-2026-4253 · GCVE-100-351211

TENDA AC8 16.03.50.11 WEB INTERFACE /CGI-BIN/UPLOADCFG ROUTE_SET_USER_POLICY_RULE WANS.POLICY.LIST1 OS COMMAND INJECTION

CVSS Meta Temp Score

5.4

Current Exploit Price (≈)

$0-$5k

CTI Interest Score

0.22

Summary

A vulnerability was found in Tenda AC8 16.03.50.11. It has been rated as critical. This vulnerability affects the function `route_set_user_policy_rule` of the file */cgi-bin/UploadCfg* of the component *Web Interface*. This manipulation of the argument *wans.policy.list1* causes os command injection. This vulnerability is handled as CVE-2026-4253. The attack can be initiated remotely. Additionally, an exploit exists.

Details

A vulnerability has been found in Tenda AC8 16.03.50.11 and classified as critical. Affected by this vulnerability is the function `route_set_user_policy_rule` of the file */cgi-bin/UploadCfg* of the component *Web Interface*. The manipulation of the argument `wans.policy.list1` with an unknown input leads to a os command injection vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-4253. The exploitation appears to be easy. The attack can be launched remotely. The exploitation needs additional levels of successful authentication. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1202 according to MITRE ATT&CK.

It is possible to download the exploit 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.

Entries connected to this vulnerability are available at VDB-347277, VDB-347400 and VDB-352404.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- AC8

Version

- 16.03.50.11

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: 5.5
VulDB Meta Temp Score: 5.4

VulDB Base Score: 4.7
VulDB Temp Score: 4.3
VulDB Vector: 🔒
VulDB Reliability: 🔍

NVD Base Score: 7.2
NVD Vector: 🔒

CNA Base Score: 4.7
CNA Vector: 🔒

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: 🔒
Access: Public

Status: Proof-of-Concept
Programming Language: 🔒
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

03/16/2026		Advisory disclosed
03/16/2026	+0 days	VulDB entry created
03/21/2026	+5 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-4253 (🔒)
GCVE (CVE): GCVE-0-2026-4253
GCVE (VulDB): GCVE-100-351211

scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/16/2026 07:21 AM
Updated: 03/21/2026 02:09 PM
Changes: 03/16/2026 07:21 AM (58), 03/21/2026 02:09 PM (41)
Complete: 🔍
Submitter: DigitalAndrew
Cache ID: 52:C83:179

Submit

Accepted

- Submit #771771: Tenda AC8 V5 V16.03.50.11 OS Command Injection (by DigitalAndrew)

Discussion

No comments yet. Languages: en.

Please log in to comment.