Tenda AC9 cross-site request forgery

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-5900
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-09 22:15:22 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability, which was classified as problematic, was found in Tenda AC9 15.03.02.13. This affects an unknown part. Th

Risk And Classification

Primary CVSS: v4.0 2.1 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-352 | CWE-862 | CWE-352 Cross-Site Request Forgery | CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/C..
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H
3.1	cna@vuldb.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:X/RC:R
3.0	CNA	DECLARED	4.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	5		AV:N/AC:L/Au:N/C:N/I:P/A:N
2.0	CNA	DECLARED	5		AV:N/AC:L/Au:N/C:N/I:P/A:N/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N/E:P/RL:X/RC:R

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tenda	Ac9	-	All	All	All
Operating System	Tenda	Ac9 Firmware	15.03.2.13	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tenda	AC9	affected 15.03.02.13	Not specified

References

Reference	Source
vuldb.com	cna@vuldb.com
candle-throne-f75.notion.site/Tenda-AC9-fromSysToolReboot-20adf0aa1185806a9d20ee5c355c08a6	cna@vuldb.com
www.tenda.com.cn	cna@vuldb.com
candle-throne-f75.notion.site/Tenda-AC9-fromSysToolRestoreSet-20adf0aa11858094a25ae21f9b4203da	134c704f-9b21-4f2e-91b3-4a4673
vuldb.com	cna@vuldb.com
vuldb.com	cna@vuldb.com
vuldb.com	cna@vuldb.com
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: ysnysn0121 (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-06-09T00:00:00.000Z	Advisory disclosed
CNA	2025-06-09T02:00:00.000Z	VulDB entry created
CNA	2025-06-09T09:47:36.000Z	VulDB entry last update

There are currently no legacy QID mappings associated with this CVE.