Arbitrary File Reading Vulnerability in dnsmasq Module in TP-Link AX53

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

Summary

CVE	CVE-2026-30817
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 19:25:20 UTC
Updated	2026-04-14 16:19:59 UTC
Description	An external configuration control vulnerability in the OpenVPN module of TP-Link AX53 v1.0 allows an authenticated adjace

Risk And Classification

Primary CVSS: v4.0 6.8 MEDIUM from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/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

EPSS: 0.000260000 probability, percentile 0.071930000 (date 2026-04-15)

Problem Types: CWE-15 | CWE-610 | CWE-15 CWE-15 External control of system or configuration setting

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	6.8	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA
4.0	CNA	CVSS	6.8	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA
3.1	nvd@nist.gov	Primary	5.7	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/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

Adjacent

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Archer Ax53	1.0	All	All	All
Operating System	Tp-link	Archer Ax53 Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	AX53 V1.0	affected 1.7.1 Build 20260213 custom	Not specified

References

Reference	Source	Link	Tags
talosintelligence.com/vulnerability_reports	f23511db-6c3e-4e32-a477-6aa17d310630	talosintelligence.com	Third Party Advi
www.tp-link.com/my/support/download/archer-ax53/v1	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
www.tp-link.com/en/support/download/archer-ax53/v1	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
www.tp-link.com/us/support/faq/5055	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

CNA: Lilith >_> of Cisco Talos (en)

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