Logic Vulnerability on TP-Link Archer C20 and Archer AX53

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

Summary

CVE	CVE-2026-0834
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-21 18:16:24 UTC
Updated	2026-04-22 22:16:30 UTC
Description	Logic vulnerability in TP-Link Archer C20 v6.0 and Archer AX53 v1.0 (TDDP module) allows unauthenticated adjacent attac

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/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: 0.000080000 probability, percentile 0.008100000 (date 2026-04-22)

Problem Types: CWE-290 | CWE-290 CWE-290 Authentication Bypass by Spoofing

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	7.2	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/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

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Archer Ax53	-	All	All	All
Operating System	Tp-link	Archer Ax53 Firmware	1.0	All	All	All
Hardware	Tp-link	Archer C20	-	All	All	All
Operating System	Tp-link	Archer C20 Firmware	6.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	Archer C20 V6.0 Archer AX53 V1.0	affected V6_251031 custom	Not specified
CNA	TP-Link Systems Inc.	Archer C20 V6.0 Archer AX53 V1.0	affected V1_251215 custom	Not specified
CNA	TP-Link Systems Inc.	Archer C20 V5	affected US_V5_260419 custom	Not specified
CNA	TP-Link Systems Inc.	Archer C20 V5	affected EU_V5_260317 custom	Not specified

References

Reference	Source	Link	Tags
www.tp-link.com/en/support/download/archer-c20/v6	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
www.tp-link.com/us/support/download/archer-c20/v5	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
www.tp-link.com/en/support/download/archer-c20/v5	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
mattg.systems/posts/cve-2026-0834	f23511db-6c3e-4e32-a477-6aa17d310630	mattg.systems	Permissions Require
www.tp-link.com/us/support/faq/4905	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
www.tp-link.com/en/support/download/archer-ax53/v1	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Matt Graham (mattg.systems) (en)

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