Hardcoded DES Decryption Keys in TP-Link Archer C50 V3/V4/V5 and C20 V5

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

Summary

CVE	CVE-2025-6982
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-16 20:15:26 UTC
Updated	2026-04-22 22:16:29 UTC
Description	Use of Hard-coded Credentials in TP-Link Archer C50 V3(<= 180703)/V4(<= 250117)/V5(<= 200407), and C20 V5 (<US

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/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: 0.000340000 probability, percentile 0.097940000 (date 2026-04-22)

Problem Types: CWE-798 | CWE-798 CWE-798 Use of Hard-coded Credentials

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	6.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

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:L/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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	Archer C50 V3	affected 180703 date	Not specified
CNA	TP-Link Systems Inc.	Archer C50 V4	affected 250117 date	Not specified
CNA	TP-Link Systems Inc.	Archer C50 V5	affected 200407 date	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/us/support/faq/4538	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
www.kb.cert.org/vuls/id/554637	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org	
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	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report