Unauthenticated Access to connectAP API Endpoint on Tapo C100 and C200

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-14300
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-20 01:16:03 UTC
Updated	2026-04-03 22:16:24 UTC
Description	The HTTPS service on Tapo C200 V3 exposes a connectAP interface without proper authentication. An unauthenticated at

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/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: 0.001030000 probability, percentile 0.283090000 (date 2026-04-03)

Problem Types: CWE-306 | CWE-306 CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	8.7	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

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:H/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

None

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Tapo C200	3	All	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.3.11	build_231115	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.3.13	build_240327	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.3.14	build_240513	All	All

Operating System	Tp-link	Tapo C200 Firmware	1.3.15	build_240715	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.3.3	build_230228	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.3.4	build_230424	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.3.5	build_230717	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.3.7	build_230920	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.3.9	build_231019	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.4.1	build_241212	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.4.2	build_250313	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.4.4	build_250922	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	Tapo C200 V3	affected V3_1.4.5 Build 251104 custom	Not specified
CNA	TP Link Systems Inc.	Tapo C100 V5	affected V5_1.4.4 Build 260303 custom	Not specified

References

Reference	Source	Link	Tags
www.tp-link.com/us/support/faq/4849	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Vendor Advisory
www.tp-link.com/en/support/download/tapo-c100/v5	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
www.tp-link.com/en/support/download/tapo-c200/v3	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
www.tp-link.com/us/support/download/tapo-c100/v5	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
www.tp-link.com/us/support/download/tapo-c200/v3	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Release Notes
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: Simone Margaritelli (evilsocket) (en)

CNA: Azim Javed of CRAC Learning (en)

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

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