Null Pointer Dereference in Tapo SmartCam HTTP Service on TP-Link Tapo C220 & C520WS

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

Summary

CVE	CVE-2026-0918
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-27 18:15:54 UTC
Updated	2026-04-29 01:16:02 UTC
Description	The Tapo C100 v5, C220 v1 and C520WS v2 cameras' HTTP service does not safely handle POST requests containing an

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/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: 0.000350000 probability, percentile 0.102360000 (date 2026-05-05)

Problem Types: CWE-476 | CWE-476 CWE-476 NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	7.1	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

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:N/VI:N/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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Tapo C220	1	All	All	All
Operating System	Tp-link	Tapo C220 Firmware	All	All	All	All
Hardware	Tp-link	Tapo C520ws	2	All	All	All
Operating System	Tp-link	Tapo C520ws Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	Tapo C220 V1	affected 1.4.2 Build 251112 custom	Not specified
CNA	TP-Link Systems Inc.	Tapo C520WS V2	affected 1.2.3 Build 251114 custom	Not specified
CNA	TP-Link Systems Inc.	Tapo C100 V5	affected 1.4.3 Build 251128 custom	Not specified

References

Reference	Source	Link
www.crac-learning.com/post/smart-home-security-research-cve-2026-0918-assigned	f23511db-6c3e-4e32-a477-6aa17d310630	www.crac
www.tp-link.com/en/support/download/tapo-c520ws/v2	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-li
www.tp-link.com/us/support/download/tapo-c100/v5	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-li
www.tp-link.com/en/support/download/tapo-c220/v1	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-li
www.tp-link.com/us/support/download/tapo-c220/v1.60	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-li
www.tp-link.com/us/support/download/tapo-c520ws/v2	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-li
www.tp-link.com/us/support/faq/4923	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-li
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Diogo Almeida @NeWbie (en)

CNA: Azim Javed & Ayushman Agrawal Hingorani from CRAC Learning (en)

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