Stack-based Buffer Overflow Leading to Denial of Service in TP-Link Tapo C520WS

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-34122
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-02 18:16:29 UTC
Updated	2026-04-02 18:16:29 UTC
Description	A stack-based buffer overflow vulnerability was identified in TP-Link Tapo C520WS v2.6 within a configuration handling con

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

Problem Types: CWE-121 | CWE-121 CWE-121 Stack-based buffer overflow

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:

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	Tapo C520WS V2.6	affected 1.2.4 Build 260326 Rel.24666n custom	Not specified

References

Reference	Source	Link	Tags
www.tp-link.com/us/support/faq/5047	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
www.tp-link.com/en/support/download/tapo-c520ws	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	
www.tp-link.com/us/support/download/tapo-c520ws	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.