Remote Code Execution via Stack-based Buffer Overflow in ONVIF SOAP Parser in TP-Link Tapo C200 and C520WS

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-8065
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-20 01:16:05 UTC
Updated	2026-04-02 18:16:26 UTC
Description	A stack-based buffer overflow vulnerability was identified in the ONVIF SOAP XML Parser in Tapo C200 v3 and C520WS v

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: 0.000240000 probability, percentile 0.063450000 (date 2026-04-02)

Problem Types: CWE-121 | CWE-120 | CWE-121 CWE-121 Stack-based buffer overflow

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	6.5	MEDIUM	CVSS:3.1/AV:A/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

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

None

Availability

High

CVSS:3.1/AV:A/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 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 C200(US)_V3_1.4.5 Build 251104 custom	Not specified
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/4849	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Vendor Advisory
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-c200/v3	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Release Notes
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

Vendor Comments And Credit

Discovery Credit

CNA: Simone Margaritelli (evilsocket) (en)

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

site. This site includes MITRE data granted under the following license.

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