



# 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

<b>CVE</b>	CVE-2025-8065
<b>State</b>	PUBLISHED
<b>Assigner</b>	TPLink
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-12-20 01:16:05 UTC
<b>Updated</b>	2026-04-02 18:16:26 UTC
<b>Description</b>	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/MSX/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/MSX/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	Tapo-link	Tapo C200	3	All	All	All
Operating System	Tapo-link	Tapo C200 Firmware	1.3.11	build_231115	All	All
Operating System	Tapo-link	Tapo C200 Firmware	1.3.13	build_240327	All	All

Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.3.14	build_240513	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.3.15	build_240715	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.3.3	build_230228	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.3.4	build_230424	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.3.5	build_230717	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.3.7	build_230920	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.3.9	build_231019	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.4.1	build_241212	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.4.2	build_250313	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C200 Firmware</a>	1.4.4	build_250922	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">TP-Link Systems Inc.</a>	<a href="#">Tapo C200 V3</a>	affected C200(US)_V3_1.4.5 Build 251104 custom	Not specified
CNA	<a href="#">TP-Link Systems Inc.</a>	<a href="#">Tapo C520WS V2.6</a>	affected 1.2.4 Build 260326 Rel.24666n custom	Not specified

#### References

Reference	Source	Link	Tags
<a href="http://www.tp-link.com/us/support/faq/4849">www.tp-link.com/us/support/faq/4849</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	Vendor Advisory
<a href="http://www.tp-link.com/en/support/download/tapo-c520ws">www.tp-link.com/en/support/download/tapo-c520ws</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	
<a href="http://www.tp-link.com/us/support/download/tapo-c200/v3">www.tp-link.com/us/support/download/tapo-c200/v3</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	Release Notes
<a href="http://www.tp-link.com/us/support/download/tapo-c520ws">www.tp-link.com/us/support/download/tapo-c520ws</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

#### Vendor Comments And Credit

##### Discovery Credit

**CNA:** [Simone Margaritelli \(evilsocket\)](#) (en)

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web](#)

[site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**