

er Spring Sale

EXTENDED!

Up to

60% off

Extra 10% off code: SPRING10



# Security Advisory on Vulnerabilities in Tapo C100 (CVE-2025-14300), Tapo C200 (CVE-2025-8065, CVE-2025-14299 & CVE-2025-14300) and Tapo C520WS (CVE-2025-8065)

Security Advisory

Updated 04-03-2026 21:38:55 PM

15396

## Vulnerabilities Description and Impacts:

### CVE-2025-8065: Remote Code Execution via Stack-based Buffer Overflow in ONVIF SOAP Parser in Tapo C200 v3 and Tapo C520WS v2.6

A stack-based buffer overflow vulnerability was identified in the ONVIF SOAP XML Parser. When processing XML tags with namespace prefixes, the parser fails to validate the prefix length before copying it to a fixed-size stack buffer. It allowed a crafted SOAP request with an oversized namespace prefix to cause memory corruption in stack.

An unauthenticated attacker on the same local network may exploit this flaw to enable remote code execution with elevated privileges, leading to full compromise of the device.

CVSS v4.0 Score: 8.7 / High

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

### CVE-2025-14299: Improper Content-Length Validation in HTTPS Requests in Tapo C200 v3

- The HTTPS server does not properly validate the Content-Length header, which could lead to an Integer Overflow.
- An unauthenticated attacker on the same local network segment can send crafted HTTPS requests to crash the device, resulting in DoS.

CVSS v4.0 Score: 7.1 / High

Welcome to Our Website! If you stay on our site, we and our third-party partners use cookies, pixels, and other tracking technologies to better understand how you use our services, and improve our services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).



Okay

- An unauthenticated attacker on the same local network segment can modify the device's Wi-Fi configuration, resulting in loss of connectivity and DoS.

CVSS v4.0 Score: 8.7 / High

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

#### Affected Products/Versions and Fixes:

Affected Product Model	Related Vulnerabilities	Affected Version
Tapo C100 v5	CVE-2025-14300	< V5_1.4.4 Build 260303
Tapo C520WS v2.6	CVE-2025-8065	< 1.2.4 Build 260326 Rel.24666n
Tapo C200 v3	CVE-2025-8065 CVE-2025-14299 CVE-2025-14300	< V3_1.4.5 Build 251104

#### Recommendations:

We strongly recommend that users with affected devices take the following actions:

1. Check and Update on Tapo Mobile Application to fix the vulnerabilities.

US: [Download for Tapo C100 | TP-Link](#)

[Download for Tapo C200 | TP-Link](#)

[Download for Tapo C520WS | TP-Link](#)

EN: [Download for Tapo C100 | TP-Link](#)

[Download for Tapo C200 | TP-Link](#)

[Download for Tapo C520WS | TP-Link](#)

#### Disclaimer:

If you do not take all of the recommended actions, this vulnerability concern will remain. TP-Link will not bear any responsibility for the consequences that could have been avoided by following the recommended actions in this advisory.

## Looking for More

Welcome to Our Website! If you stay on our site, we and our third-party partners use cookies, pixels, and other tracking technologies to better understand how you use our services, and improve our services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).



## Is this faq useful?

Your feedback helps improve this site.

Yes
  No



## TP-Link Community

Still need help? Search for answers, ask questions, and get help from TP-Link experts and other users around the world.

[Visit the Community >](#)

### Subscribe (i)

Be The First To Get Exclusive Deals & News

### Let's Connect



#### About

- About Us
- Corporate Information
- Contact Us
- Sustainability
- Privacy Policy
- Your Privacy Choices
- Careers at TP-Link
- Accessibility

#### Press

- News
- Blog
- Security Advisory
- Security News
- Awards

#### Partners

- Partner Program
- Partner Deal Registration
- MAP Policy

#### Learning Center

- Technology Trends
- Training & Certification

Welcome to Our Website! If you stay on our site, we and our third-party partners use cookies, pixels, and other tracking technologies to better understand how you use our products and services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).





©2026 TP-Link Systems Inc. and its affiliated companies. All rights reserved.


 United States / English

TP-Link, Tapo, Kasa, Omada, VIGI, Aginet, HomeShield, and Tapo Care branded products are products of TP-Link Systems Inc. or its affiliates.

Note: Some services and materials may require you to accept additional terms and conditions before access or use.

References to "TP-Link" may include TP-Link Systems Inc., its subsidiaries, or business units within the TP-Link corporate structure, as applicable.

The materials provided, including but not limited to press releases, presentations, blog posts, and webcasts, are current as of the date of publication and may be superseded by subsequent updates.

Welcome to Our Website! If you stay on our site, we and our third-party partners use cookies, pixels, and other tracking technologies to better understand how you use our  provide and improve our services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).