tp-link

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 19767

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

- 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

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

Be The First To Get Exclusive Deals & News

Email Address | Subscribe

Let's Connect