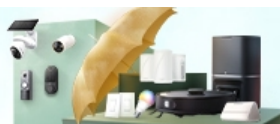


Free Showers of Savings

EXTENDED - Ends 4/30!

Savings up to
50% OFF!

Show

[Home](#) > [Support](#) > [Security Advisory](#) >

Security Advisory on Multiple Vulnerabilities on Tapo C100, C220 and C520WS (CVE-2026-0918, CVE-2026-0919 & CVE-2026-1315)

Security Advisory on Multiple Vulnerabilities on Tapo C100, C220 and C520WS (CVE-2026-0918, CVE-2026-0919 & CVE-2026-1315)

Security Advisory

Last updated: April 28, 2026

Description of Vulnerabilities and Impacts:

CVE-2026-0918: Null Pointer Dereference in Tapo SmartCam HTTP Service

In Tapo C100 v5, C220 v1 and C520WS v2, the camera's HTTP service does not safely handle POST requests containing an excessively large Content-Length header. The resulting failed memory allocation triggers a NULL pointer dereference, causing the main service process to crash.

An unauthenticated attacker can repeatedly crash the service, causing temporary denial of service. The device restarts automatically, and repeated requests can keep it unavailable.

CVE-2026-0919: Unauthenticated Denial of Service via Oversized URL in HTTP Parser

The HTTP parser in Tapo C220 v1 and C520WS v2 improperly handles requests containing an excessively long URL path. An invalid-URL error path continues into cleanup code that assumes allocated buffers exist, leading to a crash and service restart.

An unauthenticated attacker can force repeated service crashes or device reboots, causing denial of service.

CVE-2026-1315: Unauthenticated Denial of Service via Firmware Update Endpoint

By sending crafted files to the firmware update endpoint, the device (Tapo C220 v1 and C520WS v2) terminates core system services before verifying authentication or firmware integrity.

An unauthenticated attacker can trigger a persistent denial of service, requiring a manual reboot or application-initiated restart to restore normal device operation.

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

Affected Products/Versions and Fixes:

Affected Product Model	CVE-IDs	Affected Version
Tapo C220 v1	CVE-2026-0918,	< 1.4.2 Build 251112
Tapo C520WS v2	CVE-2026-0919, CVE-2026-1315	<1.2.3 Build 251114
Tapo C100 v5	CVE-2026-0918	< 1.4.3 Build 251128

Recommendations:

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

1. Download and update to the latest firmware version to fix the vulnerabilities.

US: <https://www.tp-link.com/us/support/download/tapo-c220/v1.60/>

<https://www.tp-link.com/us/support/download/tapo-c520ws/v2/>

<https://www.tp-link.com/us/support/download/tapo-c100/v5/>

EN: <https://www.tp-link.com/en/support/download/tapo-c220/v1/>

<https://www.tp-link.com/en/support/download/tapo-c520ws/v2/>

Disclaimer:

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

Related FAQs

[Statement on Archer AX21 Remote Code Execution Vulnerability\(CVE-2023-1389\)](#)

[Statement on LAN Command Execution on Archer C5400X\(CVE-2024-5035\)](#)

[Statement on Hardcoded DES Decryption Keys in TP-Link Archer C50 V3/V4/V5 and C20 V5.\(CVE-2025-6982\)](#)

[Statement on Authenticated RCE by CWMP binary.\(CVE-2025-9961\)](#)

[Statement on Root Access via UART on Tapo D230S1.\(CVE-2025-10991\)](#)

[Statement on OS command injection vulnerabilities on Omada gateways.\(CVE-2025-6541 and](#)

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](#).



[Making Hotel WiFi Secure and Easy to Use](#)

[What Is Home Network Security and How Do I Secure My WiFi Router?](#)

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



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](#).



About

Press

Partners

Learning Center

About Us

News

Partner Program

Technology Trends

Corporate Information

Blog

Partner Deal Registration

Training & Certification

Contact Us

Security Advisory

MAP Policy

Sustainability

Security News

Privacy Policy

Awards

Your Privacy Choices

Careers at TP-Link

Accessibility

Our Security Commitment

Promotions



©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 products and services, and personalize your experience and ads based on your interests. Learn more in [your privacy choices](#).

