Security Advisory on Multiple Vulnerabilities on Tapo C100, C210, C220 and C520WS (CVE-2026-0918, CVE-2026-0919 & CVE-2026-1315)

Security Advisory

Last updated: April 29, 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 C210 v3, 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.

Affected Products/Versions and Fixes:

Affected Product Model	CVE-IDs	Affected Version
Tapo C220 v1 Tapo C520WS v2	CVE-2026-0918, CVE-2026-0919, CVE-2026-1315	< 1.4.2 Build 251112 <1.2.3 Build 251114
Tapo C100 v5	CVE-2026-0918	< 1.4.3 Build 251128
Tapo C210 v3	CVE-2026-0919	<1.2.6 Build 260328

Recommendations:

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

1. Follow the instructions to 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/

   https://www.tp-link.com/us/support/download/tapo-c210/v3/

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

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

   https://www.tp-link.com/en/support/download/tapo-c210/v3/

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 OS command injection vulnerabilities on Omada gateways (CVE-2025-6541 and CVE-2025-6542)

Looking For More

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

Be The First To Get Exclusive Deals & News

Email Address | Subscribe

Let's Connect