مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Multiple Vulnerabilities in TP-Link Tapo Cameras

Tracking #:432318714

Date:03-04-2026



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple high-severity vulnerabilities have been identified in the TP-Link Tapo C520WS smart cameras. These issues include heap-based and stack-based buffer overflows, an authentication bypass flaw, and HTTP path parsing weaknesses.

## TECHNICAL DETAILS:

**Vulnerability Details**

1. CVE-2026-34118 to CVE-2026-34120: Heap-Based Buffer Overflow Vulnerabilities Leading to Denial-of- Service CVSS v4.0 Score: 7.1/ High
2. CVE ID: CVE-2026-34121 Authentication Bypass Vulnerability CVSS v4.0 Score: 8.7/ High
3. CVE-2026-34122: Stack-based Buffer Overflow Leading to Denial of Service in TP-Link Tapo C520WS CVSS v4.0 Score: 7.1/ High
4. CVE-2026-34124: Denial of Service via Path Expansion Overflow in HTTP Service CVSS v4.0 Score: 7.1/ High

Successful exploitation could allow attackers on the same network (adjacent access) to:

- Trigger Denial-of-Service (DoS) conditions
- Bypass authentication controls
- Execute unauthorized configuration changes
- Cause device crashes or reboots

The most critical vulnerability (CVE-2026-34121) enables authentication bypass, significantly increasing risk exposure.

**Affected Products:**

- Product: TP-Link Tapo C520WS
- Affected Versions: < 1.2.4 Build 260326 Rel.24666n
- Patched Version: ≥ 1.2.4 Build 260326 Rel.24666n

## RECOMMENDATIONS:

**Immediate Actions:**

- Upgrade firmware immediately to fixed version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://www.tp-link.com/us/support/faq/5047/