

er Spring Sale

EXTENDED!

Up to

60% off

Extra 10% off code: SPRING10



# Security Advisory on Multiple Vulnerabilities on Tapo C260, D235 and C520WS (CVE-2026-0651, CVE-2026-0652, CVE-2026-0653)

Security Advisory

Updated 04-02-2026 17:26:33 PM

7469

## Description of Vulnerabilities and Impacts:

### CVE-2026-0651: Path Traversal on Tapo D235, C260 and C520WS via Improper Normalization and URL Decoding Order

A path traversal vulnerability was identified TP-Link Tapo C260 v1, D235 v1 and C520WS v2.6 within the HTTP server's handling of GET requests. The server performs path normalization before fully decoding URL-encoded input and falls back to using the raw path when normalization fails. An attacker can exploit this logic flaw by supplying crafted, URL-encoded traversal sequences that bypass directory restrictions and allow access to files outside the intended web root.

Successful exploitation may allow authenticated attackers to get disclosure of sensitive system files and credentials, while unauthenticated attackers may gain access to non-sensitive static assets.

### **CVSS v4.0 Score: 6.9 / Medium**

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:L/SI:N/SA:N

### CVE-2026-0652: Remote Code Execution by Guest User

On TP-Link Tapo C260 v1, command injection vulnerability exists due to improper sanitization in certain POST parameters during configuration synchronization. An authenticated attacker can execute arbitrary system commands with high impact on confidentiality, integrity and availability. It may cause full device compromise.

### **CVSS v4.0 Score: 8.7 /High**

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L

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

**CVSS v4.0 Score: 7.2 /High**

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N

**Affected Products/Versions and Fixes:**

Affected Product Model	Related Vulnerabilities	Affected Version
Tapo C260 v1	CVE-2026-0651 CVE-2026-0652 CVE-2026-0653	< 1.1.9 Build 251226 Rel.55870n
Tapo D235 v1	CVE-2026-0651 CVE-2026-0653	< 1.2.2 Build 260210 Rel.27165n
Tapo C520WS v2.6	CVE-2026-0651	< 1.2.4 Build 260326 Rel.24666n

**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-c260/v1/>

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

EN: <https://www.tp-link.com/en/support/download/tapo-c260/v1/>

<https://www.tp-link.com/en/support/download/tapo-d235/>

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

Note: Tapo D235 is not sold in the US.

**Acknowledgements**

We thank **spaceraccoon** for responsibly reporting these issues to us.

**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.

## Looking for More

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](#).



[\[General\] TP-Link - Our Security Commitment](#)

## 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

### 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

About Us

Corporate Information

Contact Us

Sustainability

Privacy Policy

Your Privacy Choices

Careers at TP-Link

Accessibility

Our Security Commitment

Press

News

Blog

Security Advisory

Security News

Awards

Partners

Partner Program

Partner Deal Registration

MAP Policy

Learning Center

Technology Trends

Training & Certification

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](#).

