tp-link

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

Security Advisory Updated 03-13-2026 18:27:09 PM 7010

Description of Vulnerabilities and Impacts:

CVE-2026-0651: Path Traversal via Local https

On TP-Link Tapo C260 v1, path traversal is possible due to improper handling of specific GET request paths via https, allowing local unauthenticated probing of filesystem paths. An attacker on the local network can determine whether certain files exist on the device, with no read, write or code execution possibilities.

CVSS v4.0 Score: 5.3 / Medium

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/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

CVE-2026-0653: Insecure Access Control

On TP-Link Tapo C260 v1, a guest-level authenticated user can bypass intended access restrictions by sending crafted requests to a synchronization endpoint. This allows modification of protected device settings despite limited privileges. An attacker may change sensitive configuration parameters without authorization, resulting in unauthorized device state manipulation but not full code execution.

Affected Product Model	Related Vulnerabilities	Affected Version
Tapo C260 v1	CVE-2026-00651 CVE-2026-00652 CVE-2026-00653	< 1.1.9 Build 251226 Rel.55870n
Tapo D235 v1	CVE-2026-00651 CVE-2026-00653	< 1.2.2 Build 260210 Rel.27165n

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/

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

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

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

[General] TP-Link - Security Advisory

[General] TP-Link Security News

[General] TP-Link - Our Security Commitment

Is this faq useful?

Your feedback helps improve this site.

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

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.