



# Path Traversal on TP-Link Tapo D235 and C260 via Local https

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-0651
<b>State</b>	PUBLISHED
<b>Assigner</b>	TPLink
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-10 18:16:21 UTC
<b>Updated</b>	2026-04-02 18:16:26 UTC
<b>Description</b>	A path traversal vulnerability was identified TP-Link Tapo C260 v1, D235 v1 and C520WS v2.6 within the HTTP server's ha

## Risk And Classification

**Primary CVSS:** v4.0 6.9 MEDIUM from f23511db-6c3e-4e32-a477-6aa17d310630

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000950000 probability, percentile 0.265010000 (date 2026-04-02)

**Problem Types:** CWE-22 | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	6.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

None

Sub Availability

None

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Tp-link</a>	<a href="#">Tapo C260</a>	1	All	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Tapo C260 Firmware</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">TP-Link Systems Inc.</a>	<a href="#">Tapo C260 V1</a>	affected 1.1.9 Build 251226 Rel.55870n custom	Not specified
CNA	<a href="#">TP-Link Systems Inc.</a>	<a href="#">Tapo D235 V1</a>	affected 1.2.2 Build 260210 Rel.27165n custom	Not specified
CNA	<a href="#">TP Link Systems Inc.</a>	<a href="#">Tapo C520WS V2.6</a>	affected 1.2.4 Build 260326 Rel.24666n custom	Not specified

## References

Reference	Source	Link	Tags
<a href="http://www.tp-link.com/us/support/faq/4960">www.tp-link.com/us/support/faq/4960</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	Vendor Advisory
<a href="http://www.tp-link.com/us/support/download/tapo-c260/v1">www.tp-link.com/us/support/download/tapo-c260/v1</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	Product
<a href="http://www.tp-link.com/en/support/download/tapo-d235">www.tp-link.com/en/support/download/tapo-d235</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	
<a href="http://www.tp-link.com/us/support/download/tapo-c520ws">www.tp-link.com/us/support/download/tapo-c520ws</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	
<a href="http://www.tp-link.com/en/support/download/tapo-c260/v1">www.tp-link.com/en/support/download/tapo-c260/v1</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	Product
<a href="http://www.tp-link.com/en/support/download/tapo-c520ws">www.tp-link.com/en/support/download/tapo-c520ws</a>	f23511db-6c3e-4e32-a477-6aa17d310630	<a href="http://www.tp-link.com">www.tp-link.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**CNA:** spaceraccoon (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)