



# CVE-2022-41505

Published on: Not Yet Published

Last Modified on: 01/31/2023 07:10:00 PM UTC

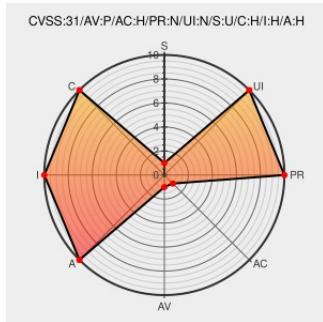
## CVE-2022-41505

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Tapo C200 V1** from **Tp-link** contain the following vulnerability:

An access control issue on TP-Link Tapo C200 V1 devices allows physically proximate attackers to obtain root access by connecting to the UART pins, interrupting the boot process, and setting an `init=/bin/sh` value.

CVE-2022-41505 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>PHYSICAL</b>	<b>HIGH</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

## CVE References

Description	Tags	Link
GitHub - hemant70072/Access-control-issue-in-TP-Link-Tapo-C200-V1.: Exploiting the UART shell to get the access of root shell and dumping the content of flash chip (firmware) in the SD card	<a href="https://github.com">github.com</a> <a href="#">text/html</a>	<a href="https://github.com/hemant70072/Access-control-issue-in-TP-Link-Tapo-C200-V1">MISC github.com/hemant70072/Access-control-issue-in-TP-Link-Tapo-C200-V1.</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).


There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Tapo-link	Tapo C200 V1	-	All	All	All
Operating System	Tapo-link	Tapo C200 V1 Firmware	-	All	All	All
cpe:2.3:h:tp-link:tapo_c200_v1:-:*:*:*:*:*:						
cpe:2.3:o:tp-link:tapo_c200_v1_firmware:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVereport	CVE-2022-41505 : An access control issue on TP-Link Tapo C200 V1 devices allows physically proximate attackers to o... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2023-01-23 15:20:17
 /r/netcve	<a href="#">CVE-2022-41505</a>	2023-01-23 15:39:29

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)**