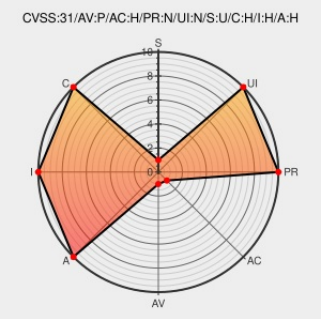
CVE-2022-41505

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 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
PHYSICAL	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

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	github.com text/html	MISC github.com/hemant70072/Access-control-issue-in-TP-Link-Tapo-C200-V1.

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	Tp-link	Tapo C200 V1	-	All	All	All
Operating System	Tp-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… twitter.com/i/web/status/1…	2023-01-23 15:20:17
/r/netcve	CVE-2022-41505	2023-01-23 15:39:29

← Previous ID

Next ID→