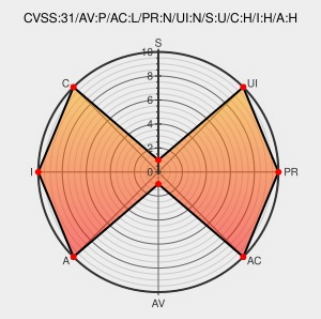
CVE-2020-27542

Published on: 01/25/2021 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-27542

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cs-c2shw from Company contain the following vulnerability:

Rostelecom CS-C2SHW 5.0.082.1 is affected by: Bash command injection. The camera reads configuration from QR code (including network settings). The static IP configuration from QR code is copied to the file /config/ip-static and after reboot data from this file is inserted into bash command (without any escaping). So bash injection is possible. Camera doesn't parse QR codes if it's already successfully configured. Camera is always rebooted after successful configuration via QR code.

CVE-2020-27542 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Groundhog Day in IoT Valley, or 5 CVEs in 1 Camera | by	Exploit	MISC dil4rd.medium.com/groundhog-day-in-iot

Groundhog Day in IoT Valley, or 5 CVEs in 1 Camera | by Andrey Lovyannikov | Medium	Exploit Third Party Advisory dil4rd.medium.com text/html	MISC dil4rd.medium.com/groundhog-day-in-iot-valley-or-5-cves-in-1-camera-7dc1d2864707

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Company	Cs-c2shw	-	All	All	All
Hardware	Company	Cs-c2shw	-	All	All	All
Operating System	Company	Cs-c2shw Firmware	5.0.082.1	All	All	All
Operating System	Company	Cs-c2shw Firmware	5.0.082.1	All	All	All

cpe:2.3:h:company:cs-c2shw:-:*:*:*:*:*:*:*:

cpe:2.3:h:company:cs-c2shw:-:*:*:*:*:*:*:*:

cpe:2.3:o:company:cs-c2shw_firmware:5.0.082.1:*:*:*:*:*:*:*:

cpe:2.3:o:company:cs-c2shw_firmware:5.0.082.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→