CVE-2020-27540

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-27540
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 18:15:00 UTC
Updated	2021-02-02 18:53:00 UTC
Description	Bash injection vulnerability and bypass of signature verification in Rostelecom CS-C2SHW 5.0.082.1. The camera reads firı

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Groundhog Day in IoT Valley, or 5 CVEs in 1 Camera | by Andrey Lovyannikov | Medium	MISC	dil4rd.medium.com	Exploit, Third P
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report