

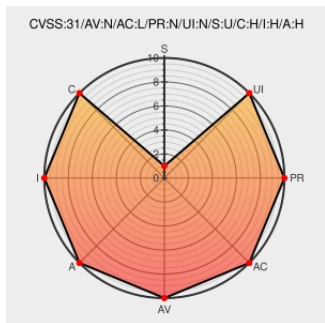


CVE-2020-27539

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

Last Modified on: 03/23/2021 11:23:28 PM UTC

CVE-2020-27539

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Cs-c2shw](#) from [Company](#) contain the following vulnerability:

Heap overflow with full parsing of HTTP response in Rostelecom CS-C2SHW 5.0.082.1. AgentUpdater service has a self-written HTTP parser and builder. HTTP parser has a heap buffer overflow (OOB write). In default configuration camera parses responses only from HTTPS URLs from config file, so vulnerable code is unreachable and one more bug required to reach it.

CVE-2020-27539 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	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 Andrey Lovyannikov Medium	Exploit Third Party Advisory	MISC dil4rd.medium.com/groundhog-day-in-iot-valley-or-5-cves-in-1-camera-7dc1d2864707

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.

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→