



CVE-2020-25747

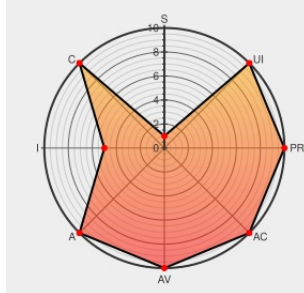
Published on: 09/24/2020 12:00:00 AM UTC

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

CVE-2020-25747

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H



Certain versions of [Rv-3406](#) from [Rubetek](#) contain the following vulnerability:

The Telnet service of Rubetek RV-3406, RV-3409, and RV-3411 cameras (firmware versions v342, v339) can allow a remote attacker to gain access to RTSP and ONVIF services without authentication. Thus, the attacker can watch live streams from the camera, rotate the camera, change some settings (brightness, clarity, time), restart the camera, or reset it to factory settings.

CVE-2020-25747 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.4 - CRITICAL**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
GitHub - jet-pentest/CVE-2020-25747: CVE-2020-25747	Third Party Advisory github.com	MISC github.com/jet-pentest/CVE-2020-25747

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

Exploit/POC from Github

CVE-2020-25747

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Rubetek	Rv-3406	-	All	All	All
Hardware 	Rubetek	Rv-3406	-	All	All	All
Operating System	Rubetek	Rv-3406 Firmware	339	All	All	All
Operating System	Rubetek	Rv-3406 Firmware	342	All	All	All
Operating System	Rubetek	Rv-3406 Firmware	339	All	All	All
Operating System	Rubetek	Rv-3406 Firmware	342	All	All	All
Hardware 	Rubetek	Rv-3409	-	All	All	All
Hardware 	Rubetek	Rv-3409	-	All	All	All
Operating System	Rubetek	Rv-3409 Firmware	339	All	All	All
Operating System	Rubetek	Rv-3409 Firmware	342	All	All	All
Operating System	Rubetek	Rv-3409 Firmware	339	All	All	All
Operating System	Rubetek	Rv-3409 Firmware	342	All	All	All
Hardware 	Rubetek	Rv-3411	-	All	All	All
Hardware 	Rubetek	Rv-3411	-	All	All	All
Operating System	Rubetek	Rv-3411 Firmware	339	All	All	All
Operating System	Rubetek	Rv-3411 Firmware	342	All	All	All
Operating System	Rubetek	Rv-3411 Firmware	339	All	All	All

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →