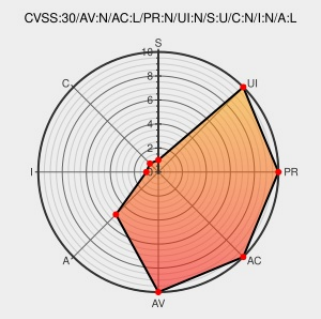
CVE-2018-4027

Published on: 05/13/2019 12:00:00 AM UTC

Last Modified on: 06/07/2022 04:48:00 PM UTC

CVE-2018-4027

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



Certain versions of Roav Dashcam A1 from Anker-in contain the following vulnerability:

An exploitable denial-of-service vulnerability exists in the XML_UploadFile Wi-Fi command of the NT9665X Chipset firmware, running on the Anker Roav A1 Dashcam, version RoavA1SWV1.9. A specially crafted packet can cause a semaphore deadlock, which prevents the device from receiving any physical or network inputs. An attacker can send a specially crafted packet to trigger this vulnerability.

CVE-2018-4027 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
TALOS-2018-0699 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory	MISC talosintelligence.com/vulnerability_reports/TALOS-

talosintelligence.com 2018-0699
text/html

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	Anker-in	Roav Dashcam A1	-	All	All	All
Hardware	Anker-in	Roav Dashcam A1	-	All	All	All
Operating System	Anker-in	Roav Dashcam A1 Firmware	1.9	All	All	All
Operating System	Anker-in	Roav Dashcam A1 Firmware	1.9	All	All	All

cpe:2.3:h:anker-in:roav_dashcam_a1:-:*:*:*:*:*:*:*:

cpe:2.3:h:anker-in:roav_dashcam_a1:-:*:*:*:*:*:*:*:

cpe:2.3:o:anker-in:roav_dashcam_a1_firmware:1.9:*:*:*:*:*:*:*:

cpe:2.3:o:anker-in:roav_dashcam_a1_firmware:1.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→