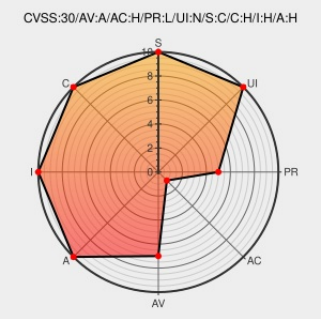
CVE-2018-4016

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

Last Modified on: 06/07/2022 04:41:00 PM UTC

CVE-2018-4016

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



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

An exploitable code execution vulnerability exists in the URL-parsing functionality of the Roav A1 Dashcam running version RoavA1SWV1.9. A specially crafted packet can cause a stack-based buffer overflow, resulting in code execution. An attacker can send a packet to trigger this vulnerability.

CVE-2018-4016 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
TALOS-2018-0687 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Third Party Advisory, talosintelligence.com, text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2018-0687

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	roava1swv1.9	All	All	All
Operating System	Anker-in	Roav Dashcam A1 Firmware	roava1swv1.9	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:roava1swv1.9:*:*:*:*:*:*:*:

cpe:2.3:o:anker-in:roav_dashcam_a1_firmware:roava1swv1.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→