CVE-2023-0847

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-0847
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-01 00:15:00 UTC
Updated	2023-11-07 04:01:00 UTC
Description	The Sub-IoT implementation of the DASH 7 Alliance protocol has a vulnerability that can lead to an out-of-bounds write prio

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dash7-alliance	Dash7 Alliance Protcol	All	All	All	All

References

Reference	Source	Link	Tag
Sub-IoT DASH 7 Alliance Protocol stack implementation | CISA	MISC	www.cisa.gov	
Possible remote memory corruption over the DASH7 modem · Advisory · Sub-IoT/Sub-IoT-Stack · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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