CVE-2023-2504

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

Summary

CVE	CVE-2023-2504
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-22 22:15:00 UTC
Updated	2023-05-31 14:07:00 UTC
Description	Files present on firmware images could allow an attacker to gain unauthorized access as a root user using hard-coded crec

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Birddog	4k Quad	-	All	All	All
Operating System	Birddog	4k Quad Firmware	4.5.181	All	All	All
Operating System	Birddog	4k Quad Firmware	4.5.196	All	All	All
Hardware	Birddog	A300	-	All	All	All
Operating System	Birddog	A300 Firmware	3.4	All	All	All
Hardware	Birddog	Mini	-	All	All	All
Operating System	Birddog	Mini Firmware	2.6.2	All	All	All
Hardware	Birddog	Studio R3	-	All	All	All
Operating System	Birddog	Studio R3 Firmware	3.6.4	All	All	All

References

Reference	Source	Link	Tags
BirdDog Cameras and Encoders | CISA	MISC	www.cisa.gov	
Downloads – BirdDog	MISC	birddog.tv	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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**