



CVE-2023-38026

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-38026
State	PUBLIC
Assigner	cve@cert.org.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-28 04:15:00 UTC
Updated	2023-08-29 16:25:00 UTC
Description	SpotCam Co., Ltd. SpotCam FHD 2 has a vulnerability of using hard-coded uBoot credentials. An remote attacker can exploit this vulnerability to gain unauthorized access to the device.

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Myspotcam	Fhd 2	-	All	All	All
Operating System	Myspotcam	Fhd 2 Firmware	All	All	All	All

References

Reference
TWCERT/CC台灣電腦網路危機處理暨協調中心 企業資安通報協處 資安情資分享 漏洞通報 資安聯盟 資安電子報-視博網訊 SpotCam FHD 2 - L
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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