CVE-2023-27126

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-27126
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-06 18:15:00 UTC
Updated	2023-06-12 16:28:00 UTC
Description	The AES Key-IV pair used by the TP-Link TAPO C200 camera V3 (EU) on firmware version 1.1.22 Build 220725 is reused

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Tapo C200	3	All	All	All
Operating System	Tp-link	Tapo C200 Firmware	1.2.2	build_220725	All	All

References

Reference	Source	Link	Tags
Tapo Smart | Smart Devices for Smart Living	MISC	tapo.com	
Dans les entrailles d'une caméra connectée TP-Link (1/4) | Claranet France	MISC	www.claranet.fr	
TP-Link Canada - WiFi Networking Equipment for Home & Business	MISC	tp-link.com	
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.

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