CVE-2023-25946

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

Summary

CVE	CVE-2023-25946
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-23 02:15:00 UTC
Updated	2023-05-30 22:20:00 UTC
Description	Authentication bypass vulnerability in Qrio Lock (Q-SL2) firmware version 2.0.9 and earlier allows a network-adjacent attack

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Qrio	Q-sl2	-	All	All	All
Operating System	Qrio	Q-sl2 Firmware	All	All	All	All

References

Reference	Source	Link
JVN#48687031: Qrio Smart Lock Q-SL2 vulnerable to authentication bypass by capture-replay	MISC	jvn.jp
Qrio Lockの通信プロトコルのさらなるセキュリティ強化を実施しました | Qrio製品情報・Qrio Store | Qrio（キュリオ）	MISC	qrio.n
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

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