CVE-2021-27941

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

Summary

CVE	CVE-2021-27941
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-06 21:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	Unconstrained Web access to the device's private encryption key in the QR code pairing mode in the eWeLink mobile appli

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Coolkit	Ewelink	All	All	All	All
Application	Coolkit	Ewelink	All	All	All	All

References

Reference
eWeLink - Smart Home - Apps on Google Play
eWeLink-Smart Home on the App Store
GitHub - salgio/eWeLink-QR-Code: This repo describes a vulnerability affecting the QR code based pairing process of the eWeLink IoT device
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

630706 eWeLink - Smart Home For Android Incorrect Authorization Vulnerability

630716 eWeLink For iOS Incorrect Authorization Vulnerability

Free CVE JSON API cve.report/api

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