



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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)