



CVE-2021-38784

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-38784 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-01-18 14:15:00 UTC |
| Updated | 2022-01-26 17:32:00 UTC |
| Description | There is a NULL pointer dereference in the syscall open_exec function of Allwinner R818 SoC Android Q SDK V1.0 that co |

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-------------------------------|---|---------|--------|---------|----------|
| Application | Allwinnertech | Android Q Sdk | 1.0 | All | All | All |
| Application | Allwinnertech | Android Q Sdk Camera Driver | 1.0 | All | All | All |
| Hardware | Allwinnertech | R818 | - | All | All | All |

References

Reference

www.cnvd.org.cn/flaw/show/CNVD-2021-49172

undefined_undefined-网安漏洞平台

CPU

MY_CVE_CREDIT/Allwinner R818 SoC : Syscall open_exec has Null Pointer Dereference Vulnerability.md at master · pokerfacett/MY_CVE_

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.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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)