



CVE-2021-39714

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

Summary

CVE	CVE-2021-39714
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-16 15:15:00 UTC
Updated	2022-09-28 19:54:00 UTC
Description	In ion_buffer_kmap_get of ion.c, there is a possible use-after-free due to an integer overflow. This could lead to local escape

Risk And Classification

Problem Types: CWE-190 | CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	-	All	All	All

References

Reference	Source	Link	Tags
Pixel Update Bulletin—March 2022 Android Open Source Project	MISC	source.android.com	
Pixel Update Bulletin—August 2022 Android Open Source Project	MISC	source.android.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.

Legacy QID Mappings

[179118](#) Debian Security Update for linux (DLA 2940-1)

[180519](#) Debian Security Update for linux (CVE-2021-39714)

[610400](#) Google Pixel Android March 2022 Security Patch Missing

[610408](#) Google Android April 2022 Security Patch Missing for Huawei EMUI

© [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](#)