

CVE-2023-20963

Android Framework Privilege Escalation Vulnerability

CISA KEV since Apr 13, 2023

Actively exploited

In WorkSource, there is a possible parcel mismatch. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-11 Android-12 Android-12L Android-13 Android ID: A-220302519

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.015 73.5th percentile · FIRST	CISA DEADLINE May 4, 2023 KEV since 2023 · listed over a year
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.015 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
android	11.0 12.0 12.1 13.0	no fixed version listed	NVD

Sources

Vendor guidance	source.android.com/security/bulletin/2023-03-01	source.android.com	source.android.com/docs/security/bulletin/2023-03-01
NVD	nvd.nist.gov/vuln/detail/CVE-2023-20963	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-25131	Current data	evulnable.com/vulnerability-management/cve/CVE-2023-20963

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.