

CVE-2025-48543

Android Runtime Use-After-Free Vulnerability

CISA KEV since Sep 4, 2025

Actively exploited

In multiple locations, there is a possible way to escape chrome sandbox to attack android system_server due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

EVRS 75/100 Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.006 49.7th percentile · FIRST	CISA DEADLINE Sep 25, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.006 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
android	13.0 14.0 15.0 16.0	no fixed version listed	NVD

Sources

Vendor guidance	android.googlesource.com/platform/art/+444fc40dfb04d2ec5f74c443ed3a4dd45d3131f2	Additional guidance	source.android.com/security/bulletin/2025-09-01
source.android.com	source.android.com/docs/security/bulletin/2025-09-01	NVD	nvd.nist.gov/vuln/detail/CVE-2025-48543
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-26791
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-48543		

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