

CVE-2021-25372

Samsung Mobile Devices Improper Boundary Check Vulnerability

CISA KEV since Jun 29, 2023

Actively exploited

An improper boundary check in DSP driver prior to SMR Mar-2021 Release 1 allows out of bounds memory access.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 6.7 Medium · NVD	EPSS 0.008 56.3rd percentile · FIRST	CISA DEADLINE Jul 20, 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	0.008 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.7	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions or discontinue use of the product if updates are unavailable

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
android	10.0 11.0	no fixed version listed	NVD
exynos 2100	—	no fixed version listed	NVD
exynos 980	—	no fixed version listed	NVD
exynos 9830	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-qvjg-564f-22c8	Additional guidance	security.samsungmobile.com
security.samsungmobile.com	security.samsungmobile.com/securityUpdate.smsb?year=2021&month=3	NVD	nvd.nist.gov/vuln/detail/CVE-2021-25372
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-12268
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-25372		

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