

CVE-2021-25487

Samsung Mobile Devices Out-of-Bounds Read Vulnerability

CISA KEV since Jun 29, 2023

Actively exploited

Lack of boundary checking of a buffer in set_skb_priv() of modem interface driver prior to SMR Oct-2021 Release 1 allows OOB read and it results in arbitrary code execution by dereference of invalid function pointer.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.006 49.8th 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	0.006 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 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	8.1 9.0 10.0 11.0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-4fpw-j345-q48r

Additional guidance security.samsungmobile.com/securityUpdate.smsb?year=2021&month=10
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2021-25487

NVD nvd.nist.gov/vuln/detail/CVE-2021-25487

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2021-12383

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