

CVE-2011-1823

Android OS Privilege Escalation Vulnerability

CISA KEV since Sep 8, 2022

Actively exploited

The vold volume manager daemon on Android 3.0 and 2.x before 2.3.4 trusts messages that are received from a PF_NETLINK socket, which allows local users to execute arbitrary code and gain root privileges via a negative index that bypasses a maximum-only signed integer check in the DirectVolume::handlePartitionAdded method, which triggers memory corruption, as demonstrated by Gingerbreak.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.414 98.7th percentile · FIRST	CISA DEADLINE Sep 29, 2022 KEV since 2022 · 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	0.414 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	≥ 2.0 < 2.3.4 3.0	2.3.4	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-3hj2-5cwp-2349	android.googlesource.com	android.googlesource.com/platform/system/vold/+c51920c82463b240e2be0430849837d6fdc5352e
NVD	nvd.nist.gov/vuln/detail/CVE-2011-1823	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2011-1821	Current data	evulnable.com/vulnerability-management/cve/CVE-2011-1823

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