

CVE-2024-43093

Android Framework Privilege Escalation Vulnerability

CISA KEV since Nov 7, 2024

Actively exploited

In shouldHideDocument of ExternalStorageProvider.java, there is a possible bypass of a file path filter designed to prevent access to sensitive directories due to incorrect unicode normalization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.3 High · NVD	EPSS 0.007 53rd percentile · FIRST	CISA DEADLINE Nov 28, 2024 KEV since 2024 · 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	0.007 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch-tagged reference available; verify applicability with the vendor

CISA required action: Apply mitigations per vendor instructions 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	12.0 12.1 13.0 14.0 15.0	no fixed version listed	NVD

Sources

Vendor guidance	source.android.com/platform/frameworks/base/+7f83c671626f9bf993581f4598c22482d87cba10	source.android.com	source.android.com/docs/security/bulletin/2024-11-01
NVD	nvd.nist.gov/vuln/detail/CVE-2024-43093	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-40034	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-43093

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