CVE-2019-2215

Android Kernel Use-After-Free Vulnerability

CISA KEV since Nov 3, 2021 | Actively exploited | Public exploit module (Metasploit)

A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local application or a separate vulnerability in a network facing application.Product: AndroidAndroid ID: A-141720095

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
77/100	7.8	0.721	May 3, 2022
Urgent priority	High · NVD	99.43rd percentile · FIRST	KEV since 2021 · 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	0.721 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 · 137 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
cloud backup	–	no fixed version listed	NVD
data availability services	–	no fixed version listed	NVD
hci management node	–	no fixed version listed	NVD
service processor	–	no fixed version listed	NVD
solidfire	–	no fixed version listed	NVD
steelstore cloud integrated storage	–	no fixed version listed	NVD
android	–	no fixed version listed	NVD
debian linux	8.0	no fixed version listed	NVD

Sources

Vendor guidance	seclists.org/bugtraq/2019/Nov/11	Additional guidance	source.android.com/security/bulletin/2019-10-01
NVD	nvd.nist.gov/vuln/detail/CVE-2019-2215	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-11857	Current data	evulnable.com/vulnerability-management/cve/CVE-2019-2215

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