CVE-2019-2215

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-2215
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-11 19:15:00 UTC
Updated	2019-10-18 19:15:00 UTC
Description	A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is rec

Risk And Classification

EPSS: 0.508860000 probability, percentile 0.978870000 (date 2026-05-13)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-416

CISA Known Exploited Vulnerability

Vendor	Android
Product	Android Kernel
Name	Android Kernel Use-After-Free Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-2215

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All

References

Reference	Source	Link	Tags
Android Binder Use-After-Free ≈ Packet Storm	MISC	packetstormsecurity.com	
Bugtraq: [slackware-security] Slackware 14.2 kernel (SSA:2019-311-01)	BUGTRAQ	seclists.org	
Full Disclosure: CVE 2019-2215 Android Binder Use After Free	FULLDISC	seclists.org	

Android Security Bulletin—October 2019 | Android Open Source Project	CONFIRM	source.android.com	Vendor A
[SECURITY] [DLA 2114-1] linux-4.9 security update	MLIST	lists.debian.org	
Security Advisory - Use-after-free Vulnerability in Android Kernel	CONFIRM	www.huawei.com	
Slackware Security Advisory - Slackware 14.2 kernel Updates ≈ Packet Storm	MISC	packetstormsecurity.com	
USN-4186-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
Android Binder Use-After-Free ≈ Packet Storm	MISC	packetstormsecurity.com	
[SECURITY] [DLA 2068-1] linux security update	MLIST	lists.debian.org	
October 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**