CVE-2015-0572

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

Summary

CVE	CVE-2015-0572
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-10 10:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple race conditions in drivers/char/adsprpc.c and drivers/char/adsprpc_compat.c in the ADSPRPC driver for the Linux k

Risk And Classification

Primary CVSS: v3.1 7 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000610000 probability, percentile 0.189440000 (date 2026-05-07)

Problem Types: CWE-362 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	4.4		AV:L/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Android Security Bulletin—October 2016 | Android Open Source Project
Linux Kernel CVE-2015-0572 Privilege Escalation Vulnerability
kernel/msm - Kernel Tree for MSM/QSD family and Android on MSM/QSD
kernel/msm-3.10 - Unnamed repository
Race condition leading to arbitrary NULL write in ADSP using ioctl COMPAT_FASTRPC_IOCTL_INVOKE_FD (CVE-2015-0572) | Code Auror
CVE Program record
NVD vulnerability detail

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**