



CVE-2016-2068

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-2068
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-07-11 01:59:00 UTC
Updated	2020-07-31 14:47:00 UTC
Description	The MSM QDSP6 audio driver (aka sound driver) for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) /

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
kernel/msm-3.10 - Unnamed repository	CONFIRM	source.codeaurora.org	Mailing List,
kernel/msm-3.10 - Unnamed repository	CONFIRM	us.codeaurora.org	Mailing List,
Android Security Bulletin—July 2016 Android Open Source Project	CONFIRM	source.android.com	Patch, Vend
kernel/msm-3.18 - Unnamed repository; edit this file 'description' to name the repository.	CONFIRM	us.codeaurora.org	Mailing List,
Page not found - Code Aurora	CONFIRM	www.codeaurora.org	Broken Link
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ai

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)