



CVE-2016-5864

Published on: 08/16/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:09 PM UTC

CVE-2016-5864

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

In an audio driver function in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, some parameters are from userspace, and if they are set to a large value, integer overflow is possible followed by buffer overflow. In another function, a missing check for a lower bound may result in an out of bounds memory access.

CVE-2016-5864 has been assigned by [Q](#) product-security@qualcomm.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Q](#) **Qualcomm, Inc. - All Qualcomm products** version **Android for MSM, Firefox OS for MSM, QRD Android**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Type	Link
-------------	------	------

Description	Tags	Link
kernel/msm-4.4 - Unnamed repository	Issue Tracking Patch Third Party Advisory source.codeaurora.org text/html	 MISC source.codeaurora.org/quic/la/kernel/msm-4.4/commit/?id=cbc21ceb69cb7bca0643423a7ca982abce3ce50a
Android Security Bulletin—June 2017 Android Open Source Project	Patch Vendor Advisory source.android.com text/html	 CONFIRM source.android.com/security/bulletin/2017-06-01
Google Android Multiple Flaws Let Remote Users Deny Service, Obtain Potentially Sensitive Information, and Execute Arbitrary Code and Let Local Apps Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1038623
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report .		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	All	All	All	All
Operating System	Google	Android	All	All	All	All
cpe:2.3:o:google:android:*****:						
cpe:2.3:o:google:android:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

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