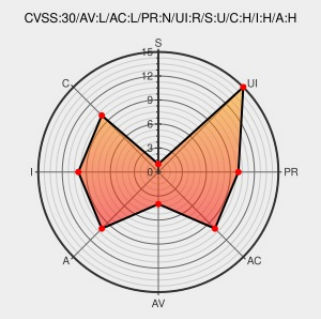
CVE-2016-5864

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 product-security@qualcomm.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **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	Tags	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

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→