

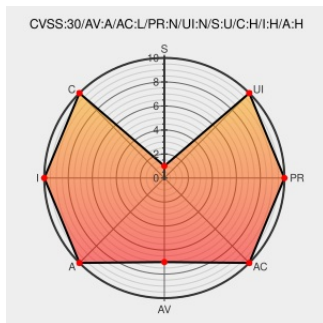


CVE-2016-5861

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

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

CVE-2016-5861

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

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

In a display driver in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, a variable controlled by userspace is used to calculate offsets and sizes for copy operations, which could result in heap overflow.

CVE-2016-5861 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: **8.8 - HIGH**

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

CVSS2 Score: **8.3 - HIGH**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Android Security Bulletin—June 2017 Android Open Source Project	Patch Vendor Advisory	CONFIRM source.android.com/security/bulletin/2017-06-01

kernel/msm-4.4 - Unnamed repository	source.android.com text/html	source.codeaurora.org/quic/la/kernel/msm-4.4/commit?id=cf3c97b8b6165f13810e530068fbf94b07f1f77d
-------------------------------------	---	---

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.

Known Affected Configurations (CPE V2.3)

No vendor comments have been submitted for this CVE

Next ID→

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