



CVE-2014-9869

Published on: 08/06/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:00 PM UTC

CVE-2014-9869

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

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

drivers/media/platform/msm/camera_v2/isp/msm_isp_stats_util.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate certain index values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28749728 and Qualcomm internal bug CR514711.

CVE-2014-9869 has been assigned by security@android.com to track the vulnerability - currently rated as **HIGH** severity.

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
Google Nexus Qualcomm Components Multiple Privilege Escalation Vulnerabilities	cve.report (archive) text/html	🌐 BID 92219
kernel/msm - Kernel Tree for MSM/OSD family	Issue Tracking	🌐 CONFIRM

kernel/msm - Kernel Tree for MSM/QSD family and Android on MSM/QSD	Issue Tracking Patch source.codeaurora.org text/html	 CONFIRM source.codeaurora.org/quic/la/kernel/msm/commit/?id=7a26934e4196b4aa61944081989189d59b108768">source.codeaurora.org/quic/la/kernel/msm/commit/?id=7a26934e4196b4aa61944081989189d59b108768
Android Security Bulletin—August 2016 Android Open Source Project	Vendor Advisory source.android.com text/html	 CONFIRM source.android.com/security/bulletin/2016-08-01.html">source.android.com/security/bulletin/2016-08-01.html
kernel/msm - Kernel Tree for MSM/QSD family and Android on MSM/QSD	Issue Tracking Patch source.codeaurora.org text/html	 CONFIRM source.codeaurora.org/quic/la/kernel/msm/commit/?id=8d1f7531ff379befc129a6447642061e87562bca">source.codeaurora.org/quic/la/kernel/msm/commit/?id=8d1f7531ff379befc129a6447642061e87562bca

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
cpe:2.3:o:google:android:*****:.*						

No vendor comments have been submitted for this CVE