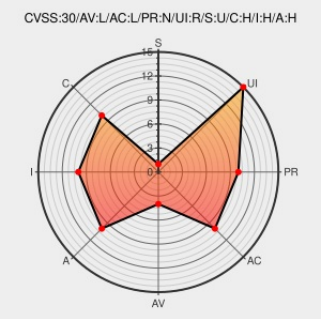
CVE-2014-9880

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

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

CVE-2014-9880

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Android from Google contain the following vulnerability:

drivers/video/msm/vidc/common/enc/venc.c in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices does not validate VEN_IOCTL_GET_SEQUENCE_HDR ioctl calls, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769352 and Qualcomm internal bug CR556356.

CVE-2014-9880 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: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

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/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=f2a3f5e63e15e97a66e8f5a300457378bcb89d9c
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

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

← Previous ID

Next ID→

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