

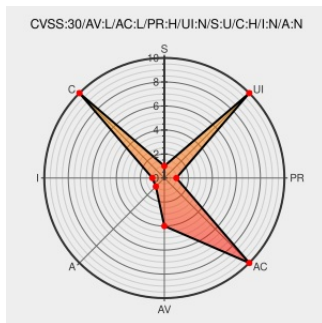


CVE-2017-15814

Published on: 03/16/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:33 PM UTC

CVE-2017-15814

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

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

In Android for MSM, Firefox OS for MSM, QRD Android, with all Android releases from CAF using the Linux kernel, in `msm_flash_subdev_do_ioctl` of `drivers/media/platform/msm/camera_v2/sensor/flash/msm_flash.c`, there is a possible out of bounds read if `flash_data.cfg_type` is

`CFG_FLASH_INIT` due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.

CVE-2017-15814 has been assigned by [Q](#) `product-security@qualcomm.com` to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description

Pixel/Nexus Security Bulletin—March 2018 | Android Open Source Project

Tags

Vendor Advisory

source.android.com

text/html

Link

 CONFIRM

source.android.com/security/bulletin/pixel/2018-03-01

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
Operating System	Google	Android	-	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 →