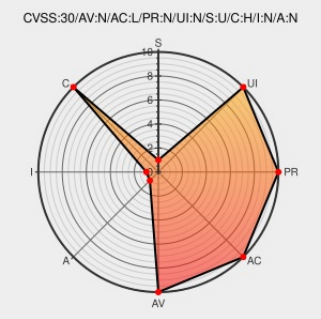
CVE-2017-9696

Published on: 11/16/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:56 PM UTC

CVE-2017-9696

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, buffer over-read is possible in camera driver function msm_isp_stop_stats_stream. Variable stream_cfg_cmd->num_streams is from userspace, and it is not checked against "MSM_ISP_STATS_MAX".

CVE-2017-9696 has been assigned by product-security@qualcomm.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Qualcomm, Inc.** - **Android for MSM, Firefox OS for MSM, QRD Android** version **All Android releases from CAF using the Linux kernel**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link

Pixel/Nexus Security Bulletin—November 2017 | Android Open Source Project	Patch Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/pixel/2017-11-01

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→