



CVE-2018-5908

Published on: 11/27/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-5908

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

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

In all android releases(Android for MSM, Firefox OS for MSM, QRD Android) from CAF using the linux kernel, there is a possible buffer overflow in display function due to lack of buffer length validation before copying.

CVE-2018-5908 has been assigned by [Q](#) product-security@qualcomm.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	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.6 - MEDIUM**

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

CVE References

Description	Tags	Link
kernel/msm-3.18 - Unnamed repository; edit this file 'description' to name the repository.	Patch Third Party Advisory source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/kernel/msm-3.18/commit/?id=28e5918c60b832091c6b3618747258803cbd3302

kernel/msm-4.4 - Unnamed repository	Patch Third Party Advisory source.codeaurora.org text/html	 CONFIRM source.codeaurora.org/quic/la/kernel/msm-4.4/commit/?id=4689d03e5db548d263232c274bf307956207da27
Page not found - Code Aurora	Patch Third Party Advisory www.codeaurora.org text/html Inactive Link Not Archived	 CONFIRM www.codeaurora.org/security-bulletin/2018/11/05/november-2018-code-aurora-forum-security-bulletin

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 →](#)