



CVE-2018-5834

Published on: 07/06/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

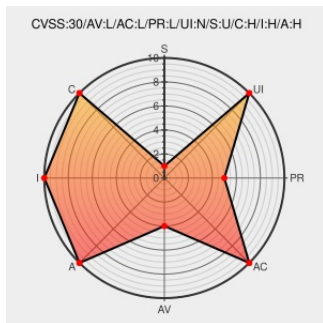
CVE-2018-5834

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In `__wlan_hdd_cfg80211_vendor_scan()`, a buffer overwrite can potentially occur in Android releases from CAF using the linux kernel (Android for MSM, Firefox OS for MSM, QRD Android) before security patch level 2018-06-05.

CVE-2018-5834 has been assigned by [Q](#) [product-security@qualcomm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

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

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
July 2018 Code Aurora Security Bulletin - Code Aurora	Patch Third Party Advisory	CONFIRM www.codeaurora.org/security-bulletin/2018/07/02/july-2018-code-aurora-security-bulletin

Confirm CVE details

Third Party Advisory

www.codeaurora.org

text/html

code aurora security confirm

platform/vendor/qcom-opensource/wlan/qcacld-3.0 - Unnamed repository

Patch

Third Party Advisory

source.codeaurora.org

text/html

CONFIRM

source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=ede0f8a4d11ec56ee87177478cc0c25af0894860

Android Security Bulletin—June 2018 | Android Open Source Project

Third Party Advisory

source.android.com

text/html

CONFIRM

source.android.com/security/bulletin/2018-06-01#qualcomm-components

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 →