



CVE-2018-5820

Published on: 04/03/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

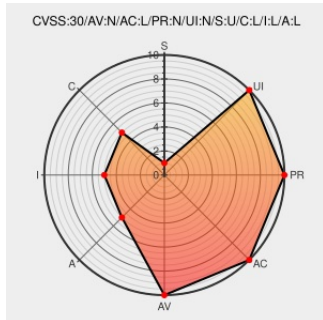
CVE-2018-5820

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In Qualcomm Android for MSM, Firefox OS for MSM, and QRD Android with all Android releases from CAF using the Linux kernel before security patch level 2018-04-05, in the function `wma_tbttoffset_update_event_handler()`, a parameter received from firmware is used to allocate memory for a local buffer and is not

properly validated. This can potentially result in an integer overflow subsequently leading to a heap overwrite.

CVE-2018-5820 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: **7.3 - HIGH**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Pixel/Nexus Security Bulletin—April 2018 Android Open Source Project	Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/pixel/2018-04-01

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

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 >