



CVE-2018-5830

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

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

CVE-2018-5830

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

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

While processing the `HTT_T2H_MSG_TYPE_MGMT_TX_COMPL_IND` message, a buffer overflow 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-2018-5830 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: **7.2 - HIGH**

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

CVE References

Description	Tags	Link
-------------	------	------

July 2018 Code Aurora Security Bulletin - Code Aurora	Third Party Advisory www.codeaurora.org/text/html	 CONFIRM www.codeaurora.org/security-bulletin/2018/07/02/july-2018-code-aurora-security-bulletin
platform/vendor/qcom-opensource/wlan/qcacld-2.0 - Unnamed repository	Patch Third Party Advisory source.codeaurora.org/text/html	 CONFIRM source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-2.0/commit/?id=8174eb0235a7e581153ea1d4a401e7ea8354cc08
Android Security Bulletin—June 2018 Android Open Source Project	Vendor Advisory source.android.com/text/html	 CONFIRM source.android.com/security/bulletin/2018-06-01#qualcomm-components
platform/vendor/qcom-opensource/wlan/qcacld-2.0 - Unnamed repository	Patch Third Party Advisory source.codeaurora.org/text/html	 CONFIRM source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-2.0/commit/?id=129e76e0ea923b319555f37ea601dfb974a06bfe

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 →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)