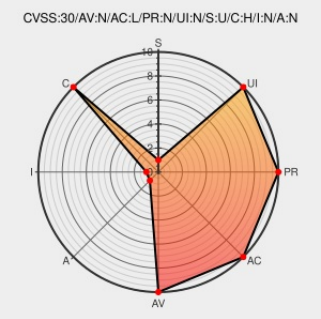
CVE-2017-18052

Published on: 03/16/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18052

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, improper input validation for cmpl_params->num_reports, param_buf->desc_ids and param_buf->status in wma_mgmt_tx_bundle_completion_handler(), which is received from firmware, leads to potential out of bounds memory read.

CVE-2017-18052 has been assigned by product-security@qualcomm.com to track the vulnerability - currently rated as HIGH severity.

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
platform/vendor/qcom-	Patch	MISC source.codeaurora.org/quic/la/platform/vendor/qcom-

opensource/wlan/qcacld-3.0 - Unnamed repository	Third Party Advisory source.codeaurora.org text/html	opensource/wlan/qcacld-3.0/commit/?id=c04c4870bd86a5f878553d7acf207388f3d6c3bd
Pixel/Nexus Security Bulletin—March 2018 | Android Open Source Project	Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/pixel/2018-03-01

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

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→