

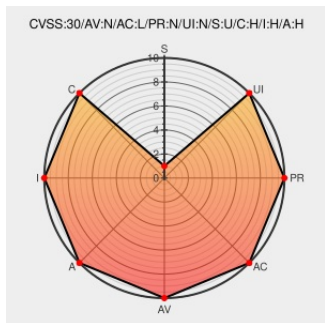


CVE-2017-14883

Published on: 03/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-14883

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

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

In the function `wma_unified_power_debug_stats_event_handler()` in Android for MSM, Firefox OS for MSM, and QRD Android before 2017-10-18, if the value `param_buf->num_debug_register` received from the FW command buffer is close to max of `uint32`, then the computation performed using this variable to calculate `stats_registers_len` may

overflow to a smaller value leading to less than required memory allocated for `power_stats_results` and potentially a buffer overflow while copying the FW buffer to local buffer.

CVE-2017-14883 has been assigned by [Q](#) product-security@qualcomm.com to track the vulnerability - currently rated as **CRITICAL** 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: **9.8 - CRITICAL**

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

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—February 2018 Android Open Source Project	Vendor Advisory source.android.com text/html	 CONFIRM source.android.com/security/bulletin/pixel/2018-02-01
platform/vendor/qcom-opensource/wlan/qcacld-3.0 - Unnamed repository	Patch Third Party Advisory source.codeaurora.org text/html	 MISC source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/qcacld-3.0/commit/?id=3de34af4e2ca91e1a2260deb380b81620a631c85

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 →