



CVE-2017-14877

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

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

CVE-2017-14877

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

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

While the IPA driver in Android for MSM, Firefox OS for MSM, and QRD Android before 2017-08-31 is processing IOCTL commands there is no mutex lock of allocated memory. If one thread sends an ioctl cmd IPA_IOC_QUERY_RT_TBL_INDEX while another sends an ioctl cmd IPA_IOC_DEL_RT_RULE, a use-after-free condition may occur.

CVE-2017-14877 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
-------------	------	------

kernel/msm-3.10 - Unnamed repository

Patch

Third Party Advisory

source.codeaurora.org

text/html

 MISC source.codeaurora.org/quic/la/kernel/msm-3.10/commit/?id=ca395c15c49cf6463a39d197b6a9331d183d94cb

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

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→