



CVE-2018-5850

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

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

CVE-2018-5850

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

In the function `csr_update_fils_params_rso()`, insufficient validation on a key length can result in an integer underflow leading to a buffer overflow in all Android releases from CAF (Android for MSM, Firefox OS for MSM, QRD Android) using the Linux Kernel.

CVE-2018-5850 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	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Android Security Bulletin—May 2018 Android Open Source Project	Patch Vendor Advisory	MISC MISC

Open Source Project

Vendor Advisory

source.android.com

text/html

May 2018 Code Aurora Security Bulletin - Code Aurora

Patch

Third Party Advisory

www.codeaurora.org

text/html

MISC

www.codeaurora.org/security-bulletin/2018/05/11/may-2018-code-aurora-security-bulletin-2

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 →