



CVE-2020-3680

Published on: 06/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3680

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

Certain versions of [Apq8009](#) from [Qualcomm](#) contain the following vulnerability:

A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130

CVE-2020-3680 has been assigned by [Q](#) product-security@qualcomm.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Q](#) **Qualcomm, Inc. - Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables** version **APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130**

CVSS3 Score: **7 - HIGH**

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

CVSS2 Score: **6.9 - MEDIUM**

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

CVE References

Description

Tags

Link

May 2020 Security Bulletin | Qualcomm

Patch

Vendor Advisory

www.qualcomm.com

text/html

 CONFIRM www.qualcomm.com/company/product-security/bulletins/may-2020-bulletin

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
Hardware 	Qualcomm	Apq8009	-	All	All	All
Hardware 	Qualcomm	Apq8009	-	All	All	All
Operating System	Qualcomm	Apq8009 Firmware	-	All	All	All
Operating System	Qualcomm	Apq8009 Firmware	-	All	All	All
Hardware 	Qualcomm	Apq8053	-	All	All	All
Hardware 	Qualcomm	Apq8053	-	All	All	All
Operating System	Qualcomm	Apq8053 Firmware	-	All	All	All
Operating System	Qualcomm	Apq8053 Firmware	-	All	All	All
Hardware 	Qualcomm	Msm8909w	-	All	All	All
Hardware 	Qualcomm	Msm8909w	-	All	All	All
Operating System	Qualcomm	Msm8909w Firmware	-	All	All	All
Operating System	Qualcomm	Msm8909w Firmware	-	All	All	All
Hardware 	Qualcomm	Msm8917	-	All	All	All
Hardware 	Qualcomm	Msm8917	-	All	All	All
Operating System	Qualcomm	Msm8917 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8917 Firmware	-	All	All	All
Hardware 	Qualcomm	Msm8953	-	All	All	All
Hardware 	Qualcomm	Msm8953	-	All	All	All

Operating System	Qualcomm	Msm8953 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8953 Firmware	-	All	All	All
Hardware 	Qualcomm	Qcs605	-	All	All	All
Hardware 	Qualcomm	Qcs605	-	All	All	All
Operating System	Qualcomm	Qcs605 Firmware	-	All	All	All
Operating System	Qualcomm	Qcs605 Firmware	-	All	All	All
Hardware 	Qualcomm	Qm215	-	All	All	All
Hardware 	Qualcomm	Qm215	-	All	All	All
Operating System	Qualcomm	Qm215 Firmware	-	All	All	All
Operating System	Qualcomm	Qm215 Firmware	-	All	All	All
Hardware 	Qualcomm	Sa415m	-	All	All	All
Hardware 	Qualcomm	Sa415m	-	All	All	All
Operating System	Qualcomm	Sa415m Firmware	-	All	All	All
Operating System	Qualcomm	Sa415m Firmware	-	All	All	All
Hardware 	Qualcomm	Sdm429	-	All	All	All
Hardware 	Qualcomm	Sdm429	-	All	All	All
Hardware 	Qualcomm	Sdm429w	-	All	All	All
Hardware 	Qualcomm	Sdm429w	-	All	All	All
Operating System	Qualcomm	Sdm429w Firmware	-	All	All	All
Operating System	Qualcomm	Sdm429w Firmware	-	All	All	All
Operating System	Qualcomm	Sdm429 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm429 Firmware	-	All	All	All
Hardware 	Qualcomm	Sdm439	-	All	All	All
Hardware 	Qualcomm	Sdm439	-	All	All	All
Operating System	Qualcomm	Sdm439 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm439 Firmware	-	All	All	All

Hardware  	Qualcomm	Sdm450	-	All	All	All
Hardware  	Qualcomm	Sdm450	-	All	All	All
Operating System	Qualcomm	Sdm450 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm450 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm632	-	All	All	All
Hardware  	Qualcomm	Sdm632	-	All	All	All
Operating System	Qualcomm	Sdm632 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm632 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm670	-	All	All	All
Hardware  	Qualcomm	Sdm670	-	All	All	All
Operating System	Qualcomm	Sdm670 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm670 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm710	-	All	All	All
Hardware  	Qualcomm	Sdm710	-	All	All	All
Operating System	Qualcomm	Sdm710 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm710 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm845	-	All	All	All
Hardware  	Qualcomm	Sdm845	-	All	All	All
Operating System	Qualcomm	Sdm845 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm845 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdx24	-	All	All	All
Hardware  	Qualcomm	Sdx24	-	All	All	All
Operating System	Qualcomm	Sdx24 Firmware	-	All	All	All
Operating System	Qualcomm	Sdx24 Firmware	-	All	All	All
Hardware  	Qualcomm	Sxr1130	-	All	All	All
Hardware  	Qualcomm	Sxr1130	-	All	All	All
Operating	Qualcomm	Sxr1130 Firmware	-	All	All	All

System						
Operating System	Qualcomm	Sxr1130 Firmware	-	All	All	All
cpe:2.3:h:qualcomm:apq8009:-:~::~:						
cpe:2.3:h:qualcomm:apq8009:-:~::~:						
cpe:2.3:o:qualcomm:apq8009_firmware:-:~::~:						
cpe:2.3:o:qualcomm:apq8009_firmware:-:~::~:						
cpe:2.3:h:qualcomm:apq8053:-:~::~:						
cpe:2.3:h:qualcomm:apq8053:-:~::~:						
cpe:2.3:o:qualcomm:apq8053_firmware:-:~::~:						
cpe:2.3:o:qualcomm:apq8053_firmware:-:~::~:						
cpe:2.3:h:qualcomm:msm8909w:-:~::~:						
cpe:2.3:h:qualcomm:msm8909w:-:~::~:						
cpe:2.3:o:qualcomm:msm8909w_firmware:-:~::~:						
cpe:2.3:o:qualcomm:msm8909w_firmware:-:~::~:						
cpe:2.3:h:qualcomm:msm8917:-:~::~:						
cpe:2.3:h:qualcomm:msm8917:-:~::~:						
cpe:2.3:o:qualcomm:msm8917_firmware:-:~::~:						
cpe:2.3:o:qualcomm:msm8917_firmware:-:~::~:						
cpe:2.3:h:qualcomm:msm8953:-:~::~:						
cpe:2.3:h:qualcomm:msm8953:-:~::~:						
cpe:2.3:o:qualcomm:msm8953_firmware:-:~::~:						
cpe:2.3:o:qualcomm:msm8953_firmware:-:~::~:						
cpe:2.3:h:qualcomm:qcs605:-:~::~:						
cpe:2.3:h:qualcomm:qcs605:-:~::~:						
cpe:2.3:o:qualcomm:qcs605_firmware:-:~::~:						
cpe:2.3:o:qualcomm:qcs605_firmware:-:~::~:						
cpe:2.3:h:qualcomm:qm215:-:~::~:						
cpe:2.3:h:qualcomm:qm215:-:~::~:						
cpe:2.3:o:qualcomm:qm215_firmware:-:~::~:						

cpe:2.3:o:qualcomm:qm215_firmware:-:*****:
cpe:2.3:o:qualcomm:qm215_firmware:-:*****:
cpe:2.3:h:qualcomm:sa415m:-:*****:
cpe:2.3:h:qualcomm:sa415m:-:*****:
cpe:2.3:o:qualcomm:sa415m_firmware:-:*****:
cpe:2.3:o:qualcomm:sa415m_firmware:-:*****:
cpe:2.3:h:qualcomm:sdm429:-:*****:
cpe:2.3:h:qualcomm:sdm429:-:*****:
cpe:2.3:h:qualcomm:sdm429w:-:*****:
cpe:2.3:h:qualcomm:sdm429w:-:*****:
cpe:2.3:o:qualcomm:sdm429w_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm429w_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm429_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm429_firmware:-:*****:
cpe:2.3:h:qualcomm:sdm439:-:*****:
cpe:2.3:h:qualcomm:sdm439:-:*****:
cpe:2.3:o:qualcomm:sdm439_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm439_firmware:-:*****:
cpe:2.3:h:qualcomm:sdm450:-:*****:
cpe:2.3:h:qualcomm:sdm450:-:*****:
cpe:2.3:o:qualcomm:sdm450_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm450_firmware:-:*****:
cpe:2.3:h:qualcomm:sdm632:-:*****:
cpe:2.3:h:qualcomm:sdm632:-:*****:
cpe:2.3:o:qualcomm:sdm632_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm632_firmware:-:*****:
cpe:2.3:h:qualcomm:sdm670:-:*****:
cpe:2.3:h:qualcomm:sdm670:-:*****:
cpe:2.3:o:qualcomm:sdm670_firmware:-:*****:

cpe:2.3:o:qualcomm:sdm670_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sdm710:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sdm710:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sdm710_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sdm710_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sdm845:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sdm845:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sdm845_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sdm845_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sdx24:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sdx24:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sdx24_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sdx24_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sxr1130:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sxr1130:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sxr1130_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sxr1130_firmware:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🔒 @hac425	add analysis of some exploits #CVE-2020-3680 #CVE-2021-22555 #CVE-2021-2119 #CVE-2022-0185 github.com/hac425xxx/heap...	2022-04-09 11:24:45

[← 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

