

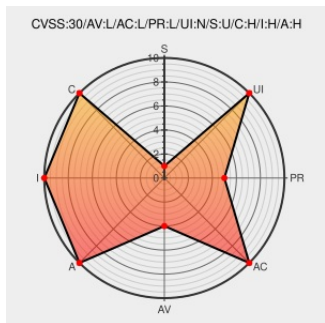


CVE-2018-5903

Published on: 06/14/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-5903

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

Certain versions of [Mdm9206](#) from [Qualcomm](#) contain the following vulnerability:

Out of bounds read occurs due to improper validation of array while processing VDEV stop response from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24

CVE-2018-5903 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music** version **MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS605, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 855, SDM630, SDM660, SDX20, SDX24**

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
May 2019 Code Aurora Security Bulletin - Code Aurora	Third Party Advisory www.codeaurora.org/text/html	 CONFIRM www.codeaurora.org/security-bulletin/2019/05/06/may-2019-code-aurora-security-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	Mdm9206	-	All	All	All
Hardware 	Qualcomm	Mdm9206	-	All	All	All
Operating System	Qualcomm	Mdm9206 Firmware	-	All	All	All
Operating System	Qualcomm	Mdm9206 Firmware	-	All	All	All
Hardware 	Qualcomm	Mdm9607	-	All	All	All
Hardware 	Qualcomm	Mdm9607	-	All	All	All
Operating System	Qualcomm	Mdm9607 Firmware	-	All	All	All
Operating System	Qualcomm	Mdm9607 Firmware	-	All	All	All
Hardware 	Qualcomm	Mdm9640	-	All	All	All
Hardware 	Qualcomm	Mdm9640	-	All	All	All
Operating System	Qualcomm	Mdm9640 Firmware	-	All	All	All
Operating System	Qualcomm	Mdm9640 Firmware	-	All	All	All
Hardware 	Qualcomm	Mdm9650	-	All	All	All
Hardware 	Qualcomm	Mdm9650	-	All	All	All
Operating System	Qualcomm	Mdm9650 Firmware	-	All	All	All
Operating System	Qualcomm	Mdm9650 Firmware	-	All	All	All
Hardware 	Qualcomm	Msm8996au	-	All	All	All

Hardware  	Qualcomm	Msm8996au	-	All	All	All
Operating System	Qualcomm	Msm8996au Firmware	-	All	All	All
Operating System	Qualcomm	Msm8996au Firmware	-	All	All	All
Hardware  	Qualcomm	Qcs405	-	All	All	All
Hardware  	Qualcomm	Qcs405	-	All	All	All
Operating System	Qualcomm	Qcs405 Firmware	-	All	All	All
Operating System	Qualcomm	Qcs405 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	Sda660	-	All	All	All
Hardware  	Qualcomm	Sda660	-	All	All	All
Operating System	Qualcomm	Sda660 Firmware	-	All	All	All
Operating System	Qualcomm	Sda660 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm630	-	All	All	All
Hardware  	Qualcomm	Sdm630	-	All	All	All
Operating System	Qualcomm	Sdm630 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm630 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm660	-	All	All	All
Hardware  	Qualcomm	Sdm660	-	All	All	All
Operating System	Qualcomm	Sdm660 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm660 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdx20	-	All	All	All
Hardware  	Qualcomm	Sdx20	-	All	All	All
Operating System	Qualcomm	Sdx20 Firmware	-	All	All	All

Operating System	Qualcomm	Sdx20 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	Sd 205	-	All	All	All
Hardware  	Qualcomm	Sd 205	-	All	All	All
Operating System	Qualcomm	Sd 205 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 205 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 210	-	All	All	All
Hardware  	Qualcomm	Sd 210	-	All	All	All
Operating System	Qualcomm	Sd 210 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 210 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 212	-	All	All	All
Hardware  	Qualcomm	Sd 212	-	All	All	All
Operating System	Qualcomm	Sd 212 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 212 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 415	-	All	All	All
Hardware  	Qualcomm	Sd 415	-	All	All	All
Operating System	Qualcomm	Sd 415 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 415 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 615	-	All	All	All
Hardware  	Qualcomm	Sd 615	-	All	All	All
Operating System	Qualcomm	Sd 615 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 615 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 616	-	All	All	All
Hardware  	Qualcomm	Sd 616	-	All	All	All

Operating System	Qualcomm	Sd 616 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 616 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 625	-	All	All	All
Hardware  	Qualcomm	Sd 625	-	All	All	All
Operating System	Qualcomm	Sd 625 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 625 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 636	-	All	All	All
Hardware  	Qualcomm	Sd 636	-	All	All	All
Operating System	Qualcomm	Sd 636 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 636 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 650	-	All	All	All
Hardware  	Qualcomm	Sd 650	-	All	All	All
Operating System	Qualcomm	Sd 650 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 650 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 652	-	All	All	All
Hardware  	Qualcomm	Sd 652	-	All	All	All
Operating System	Qualcomm	Sd 652 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 652 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 670	-	All	All	All
Hardware  	Qualcomm	Sd 670	-	All	All	All
Operating System	Qualcomm	Sd 670 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 670 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 675	-	All	All	All
Hardware  	Qualcomm	Sd 675	-	All	All	All
Operating System	Qualcomm	Sd 675 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 675 Firmware	-	All	All	All

Hardware 	Qualcomm	Sd 710	-	All	All	All
Hardware 	Qualcomm	Sd 710	-	All	All	All
Operating System	Qualcomm	Sd 710 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 710 Firmware	-	All	All	All
Hardware 	Qualcomm	Sd 712	-	All	All	All
Hardware 	Qualcomm	Sd 712	-	All	All	All
Operating System	Qualcomm	Sd 712 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 712 Firmware	-	All	All	All
Hardware 	Qualcomm	Sd 730	-	All	All	All
Hardware 	Qualcomm	Sd 730	-	All	All	All
Operating System	Qualcomm	Sd 730 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 730 Firmware	-	All	All	All
Hardware 	Qualcomm	Sd 820a	-	All	All	All
Hardware 	Qualcomm	Sd 820a	-	All	All	All
Operating System	Qualcomm	Sd 820a Firmware	-	All	All	All
Operating System	Qualcomm	Sd 820a Firmware	-	All	All	All
Hardware 	Qualcomm	Sd 835	-	All	All	All
Hardware 	Qualcomm	Sd 835	-	All	All	All
Operating System	Qualcomm	Sd 835 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 835 Firmware	-	All	All	All
Hardware 	Qualcomm	Sd 855	-	All	All	All
Hardware 	Qualcomm	Sd 855	-	All	All	All
Operating System	Qualcomm	Sd 855 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 855 Firmware	-	All	All	All
cpe:2.3:h:qualcomm:mdm9206:-:*****:						
cpe:2.3:h:qualcomm:mdm9206:-:*****:						
cpe:2.3:h:qualcomm:mdm9206:-:*****:						

```
cpe:2.3:0:qualcomm:mam9206_firmware:-:::~
```

```
cpe:2.3:o:qualcomm:mdm9206_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:mdm9607:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:mdm9607:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:mdm9607_firmware:-:*:*:*:*:*:
```

cpe:2.3:o:qualcomm:mdm9607_firmware:-:*:*:*:*:*:

```
cpe:2.3:h:qualcomm:mdm9640:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:mdm9640:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:mdm9640_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:mdm9640_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:mdm9650:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:mdm9650:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:mdm9650_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:mdm9650_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:msm8996au:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:msm8996au:-:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:msm8996au_firmware:-:*:*:*:*:*

```
cpe:2.3:o:qualcomm:msm8996au_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:qcs405:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qcs405:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qcs405_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcs405_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:sda660:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sda660:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sda660_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sda660_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm630:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm630:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm630_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm630_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdm660:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdm660:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm660_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm660_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdx20:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdx20:-:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:sdx20_firmware:-:*:*:*:*:*:

cpe:2.3:o:qualcomm:sdx20_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:sd_205:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sd 205:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd_205_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd_205_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sd_210:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sd_210:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd_210_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd_210_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sd_212:-:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd_212:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd_212_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:o:qualcomm:sd_212_firmware:-:*****:
cpe:2.3:h:qualcomm:sd_415:-:*****:
cpe:2.3:h:qualcomm:sd_415:-:*****:
cpe:2.3:o:qualcomm:sd_415_firmware:-:*****:
cpe:2.3:o:qualcomm:sd_415_firmware:-:*****:
cpe:2.3:h:qualcomm:sd_615:-:*****:
cpe:2.3:h:qualcomm:sd_615:-:*****:
cpe:2.3:o:qualcomm:sd_615_firmware:-:*****:
cpe:2.3:o:qualcomm:sd_615_firmware:-:*****:
cpe:2.3:h:qualcomm:sd_616:-:*****:
cpe:2.3:h:qualcomm:sd_616:-:*****:
cpe:2.3:o:qualcomm:sd_616_firmware:-:*****:
cpe:2.3:o:qualcomm:sd_616_firmware:-:*****:
cpe:2.3:h:qualcomm:sd_625:-:*****:
cpe:2.3:h:qualcomm:sd_625:-:*****:
cpe:2.3:o:qualcomm:sd_625_firmware:-:*****:
cpe:2.3:o:qualcomm:sd_625_firmware:-:*****:
cpe:2.3:h:qualcomm:sd_636:-:*****:
cpe:2.3:h:qualcomm:sd_636:-:*****:
cpe:2.3:o:qualcomm:sd_636_firmware:-:*****:
cpe:2.3:o:qualcomm:sd_636_firmware:-:*****:
cpe:2.3:h:qualcomm:sd_650:-:*****:
cpe:2.3:h:qualcomm:sd_650:-:*****:
cpe:2.3:o:qualcomm:sd_650_firmware:-:*****:
cpe:2.3:o:qualcomm:sd_650_firmware:-:*****:
cpe:2.3:h:qualcomm:sd_652:-:*****:
cpe:2.3:h:qualcomm:sd_652:-:*****:
cpe:2.3:o:qualcomm:sd_652_firmware:-:*****:
cpe:2.3:o:qualcomm:sd_652_firmware:-:*****:

cpe:2.3:h:qualcomm:sd_670:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_670:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_670_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_670_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_675:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_675:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_675_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_675_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_710:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_710:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_710_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_710_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_712:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_712:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_712_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_712_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_730:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_730:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_730_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_730_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_820a:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_820a:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_820a_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_820a_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_835:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_835:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_835_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_835_firmware:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:qualcomm:sd_855:-:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd_855:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd_855_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd 855 firmware:-:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← 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