



CVE-2018-11953

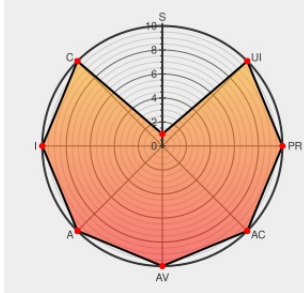
Published on: 05/24/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11953

[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 [Mdm9150](#) from [Qualcomm](#) contain the following vulnerability:

While processing ssid IE length from remote AP, possible out-of-bounds access may occur due to crafted ssid IE length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon

Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 650/52, SD 820, SD 820A, SDM439, SDX20

CVE-2018-11953 has been assigned by [Q](#) product-security@qualcomm.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Q](#) Qualcomm, Inc. - Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables version MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 650/52, SD 820, SD 820A, SDM439, SDX20

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: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact				
COMPLETE	COMPLETE	COMPLETE				
CVE References						
Description	Tags	Link				
April 2019 Code Aurora Security Bulletin - Code Aurora	Patch Third Party Advisory www.codeaurora.org text/html	 CONFIRM www.codeaurora.org/security-bulletin/2019/04/01/april-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	Mdm9150	-	All	All	All
Hardware 	Qualcomm	Mdm9150	-	All	All	All
Operating System	Qualcomm	Mdm9150 Firmware	-	All	All	All
Operating System	Qualcomm	Mdm9150 Firmware	-	All	All	All
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	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	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	Qca6174a	-	All	All	All
Hardware  	Qualcomm	Qca6174a	-	All	All	All
Operating System	Qualcomm	Qca6174a Firmware	-	All	All	All
Operating System	Qualcomm	Qca6174a Firmware	-	All	All	All
Hardware  	Qualcomm	Qca6574au	-	All	All	All
Hardware  	Qualcomm	Qca6574au	-	All	All	All
Operating System	Qualcomm	Qca6574au Firmware	-	All	All	All
Operating System	Qualcomm	Qca6574au Firmware	-	All	All	All
Hardware  	Qualcomm	Qca9377	-	All	All	All
Hardware  	Qualcomm	Qca9377	-	All	All	All
Operating System	Qualcomm	Qca9377 Firmware	-	All	All	All
Operating System	Qualcomm	Qca9377 Firmware	-	All	All	All
Hardware  	Qualcomm	Qca9379	-	All	All	All
Hardware  	Qualcomm	Qca9379	-	All	All	All

Hardware  	Qualcomm	Qca9379	-	All	All	All
Operating System	Qualcomm	Qca9379 Firmware	-	All	All	All
Operating System	Qualcomm	Qca9379 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	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	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	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

System						
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 425	-	All	All	All
Hardware  	Qualcomm	Sd 425	-	All	All	All
Operating System	Qualcomm	Sd 425 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 425 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 429	-	All	All	All
Hardware  	Qualcomm	Sd 429	-	All	All	All
Operating System	Qualcomm	Sd 429 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 429 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 439	-	All	All	All
Hardware  	Qualcomm	Sd 439	-	All	All	All
Operating System	Qualcomm	Sd 439 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 439 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 450	-	All	All	All
Hardware  	Qualcomm	Sd 450	-	All	All	All
Operating System	Qualcomm	Sd 450 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 450 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


```

CPE.2.3.11.qualcomm.mdm9605 100.0 . . . . .

```

```
cpe:2.3:h:qualcomm:mdm9150:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:mdm9150_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:mdm9150_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:mdm9206:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:mdm9206:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:mdm9206_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: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: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:gca6174a:-:*:*:*:*:*:

cpe:2.3:h:qualcomm:gca6174a:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca6174a_firmware:-:*:*:*:*:*.*
```

```
cpe:2.3:o:qualcomm:qca6174a_firmware:-:*:*:*:*:*.*
```

```
cpe:2.3:h:qualcomm:qca6574au:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qca6574au:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca6574au_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qca6574au_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:gca9377:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:gca9377:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:gca9377_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:gca9377_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:gca9379:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca9379:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca9379_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qca9379_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: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: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: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_425:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_425:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_425_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_425_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_429:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_429:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_429_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_429_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_439:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_439:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_439_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_439_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_450:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_450:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:o:qualcomm:sd_450_firmware:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:o:qualcomm:sd_450_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_632:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:h:qualcomm:sd_632:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:o:qualcomm:sd_632_firmware:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:o:qualcomm:sd_632_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_820:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:h:qualcomm:sd_820:-:~::~~::~~::~~::~~::~~::~~::~::

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:o:qualcomm:sd 820 firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd 820 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