



CVE-2019-2276

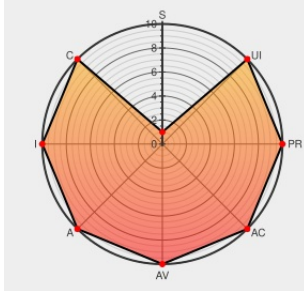
Published on: 07/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:04 PM UTC

CVE-2019-2276

[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 [Mdm9607](#) from [Qualcomm](#) contain the following vulnerability:

Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A,

QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24

CVE-2019-2276 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 Mobile, Snapdragon Voice & Music version MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24

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
July 2019 Code Aurora Security Bulletin - Code Aurora	Patch Third Party Advisory www.codeaurora.org text/html	 CONFIRM www.codeaurora.org/security-bulletin/2019/07/01/july-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	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	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	Qualcomm	-	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
Operating System	Qualcomm	Qca9379 Firmware	-	All	All	All
Operating System	Qualcomm	Qca9379 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	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	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 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 665	-	All	All	All
Hardware  	Qualcomm	Sd 665	-	All	All	All
Operating System	Qualcomm	Sd 665 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 665 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

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 845	-	All	All	All
Hardware	Qualcomm	Sd 845	-	All	All	All
Operating System	Qualcomm	Sd 845 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 845 Firmware	-	All	All	All
Hardware	Qualcomm	Sd 850	-	All	All	All
Hardware	Qualcomm	Sd 850	-	All	All	All
Operating System	Qualcomm	Sd 850 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 850 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: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: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:qca6174a:-:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca6174a:-:*:*:*:*:*:

```
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:qca9377:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca9377:-:*:*:*:*:*:*:

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

```
cpe:2.3:o:qualcomm:qca9377_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:gca9379_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:gcs605:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qcs605_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcs605_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:sd_x24:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_x24:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_x24_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_x24_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_665:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_665:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_665_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_665_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_845:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_845:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_845_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_845_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_850:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_850:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_850_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_850_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 →](#)

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](#)