



CVE-2018-3583

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

Last Modified on: 03/23/2021 11:24:26 PM UTC

CVE-2018-3583

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

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

A buffer overflow can occur while processing an extscan hotlist event in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9379, QCS605, SD 625, SD 636, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20

CVE-2018-3583 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 Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables version MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCS405, QCS605, SD 636, SD 675, SD 730, SD 820A, SD 835, SD 855, SDA660, 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
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
May 2019 Code Aurora Security Bulletin - Code Aurora	Patch 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	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	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	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	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 820	-	All	All	All
Hardware  	Qualcomm	Sd 820	-	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
Operating System	Qualcomm	Sd 820 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 820 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	Qualcomm	Sd 855 Firmware	-	All	All	All

System						
Operating System	Qualcomm	Sd 855 Firmware	-	All	All	All
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:qca9379:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:qualcomm:qca9379:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:qualcomm:qca9379_firmware:-:~::~~::~~::~~::~~::~~::~~:::						

```
0x02.0.0.gad600000.gad600 / 0_0000000 . . . . .
```

```
cpe:2.3:o:qualcomm:qca9379 firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:gcs605:-:*:*:*:*:*:
```

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

