



CVE-2018-13909

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

Last Modified on: 03/23/2021 11:24:29 PM UTC

CVE-2018-13909

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

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

Metadata verification and partial hash system calls by bootloader may corrupt parallel hashing state in progress resulting in unexpected behavior in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &

Music in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130

CVE-2018-13909 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 Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music version MDM9206, MDM9607, MDM9650, MDM9655, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, 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			
Bulletins Qualcomm	Vendor Advisory www.qualcomm.com text/html		Q CONFIRM www.qualcomm.com/company/product-security/bulletins			
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	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	Mdm9655	-	All	All	All
Hardware 	Qualcomm	Mdm9655	-	All	All	All
Operating System	Qualcomm	Mdm9655 Firmware	-	All	All	All
Operating System	Qualcomm	Mdm9655 Firmware	-	All	All	All

Operating System	Qualcomm	Qcs605 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	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	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	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	Sd 410	-	All	All	All
Hardware  	Qualcomm	Sd 410	-	All	All	All

Operating System	Qualcomm	Sd 410 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 410 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 412	-	All	All	All
Hardware  	Qualcomm	Sd 412	-	All	All	All
Operating System	Qualcomm	Sd 412 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 412 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 427	-	All	All	All
Hardware  	Qualcomm	Sd 427	-	All	All	All
Operating System	Qualcomm	Sd 427 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 427 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 430	-	All	All	All
Hardware  	Qualcomm	Sd 430	-	All	All	All
Operating System	Qualcomm	Sd 430 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 430 Firmware	-	All	All	All
Hardware  	Qualcomm	Sd 435	-	All	All	All
Hardware  	Qualcomm	Sd 435	-	All	All	All
Operating System	Qualcomm	Sd 435 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 435 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 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 632	-	All	All	All
Hardware  	Qualcomm	Sd 632	-	All	All	All
Operating System	Qualcomm	Sd 632 Firmware	-	All	All	All
Operating System	Qualcomm	Sd 632 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 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 710	-	All	All	All
Hardware  	Qualcomm	Sd 710	-	All	All	All
Operating System	Qualcomm	Sd 710 Firmware	-	All	All	All

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: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:mdm9655:-:*:*:*:*:*:

```
cpe:2.3:h:qualcomm:mdm9655:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:mdm9655_firmware:-:*:*:*:*:*.*
```

```
cpe:2.3:o:qualcomm:mdm9655_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: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: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: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: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_410:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_410:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_410_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_410_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_412:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_412:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_412_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_412_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_427:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:sd_427:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_427_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:sd_427_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_430:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:h:qualcomm:sd_430:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:o:qualcomm:sd_430_firmware:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:o:qualcomm:sd_430_firmware:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:h:qualcomm:sd_435:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:h:qualcomm:sd_435:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:o:qualcomm:sd_435_firmware:-:~::~~::~~::~~::~~::~~::~~::~::
cpe:2.3:o:qualcomm:sd_435_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_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_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_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_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_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_8cx:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sd_8cx:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sd_8cx_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sd_8cx_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:snapdragon_high_med_2016:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:snapdragon high med 2016:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:snapdragon_high_med_2016_firmware:.*:.*:.*:.*:.*:.*:.*:.*
```

cpe:2.3:o:qualcomm:snapdragon_high_med_2016_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	
← Previous ID	Next ID →