



CVE-2018-5914

Published on: 10/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:44 PM UTC

CVE-2018-5914

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

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

Improper input validation in TZ led to array out of bound in TZ function while accessing the peripheral details using the incoming data in Snapdragon Mobile, Snapdragon Wear version MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 835, SDA660.

CVE-2018-5914 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 Mobile, Snapdragon Wear** version **MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 835, SDA660**

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
-------------	------	------

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	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	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

Operating System	Qualcomm	Sd 200 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 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 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 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 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 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
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: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: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: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_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_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_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_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_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: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_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: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_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: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_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: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_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: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_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: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_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: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_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: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_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: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_835:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sd_835:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sd_835_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sd_835_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