

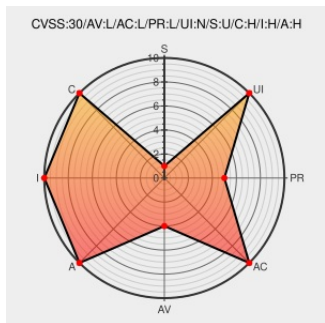


CVE-2018-11855

Published on: 02/11/2019 12:00:00 AM UTC

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

CVE-2018-11855

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

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

If an end user makes use of SCP11 sample OCE code without modification it could lead to a buffer overflow when transmitting a CAPDU in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT and

Snapdragon Mobile in versions MDM9607, MDM9650, MDM9655, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM630, SDM660.

CVE-2018-11855 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 Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile** version **MDM9607, MDM9650, MDM9655, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM630, SDM660**

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
Bulletins Qualcomm	Vendor Advisory www.qualcomm.com text/html	 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	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
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	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	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
Hardware  	Qualcomm	Sd 410	-	All	All	All
Hardware  	Qualcomm	Sd 410	-	All	All	All
Operating System	Qualcomm	Sd 410 Firmware	-	All	All	All

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: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: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:sd 205:-:*:*:*:*:*:*:
```

one:23.historicalcommid 205-*****.

Упр.2.0.11.quad00000000_200.

```
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_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_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_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:-:~::~~::~~::~~::~~::~~::~~::
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: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:-:~::~~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE