



CVE-2019-14111

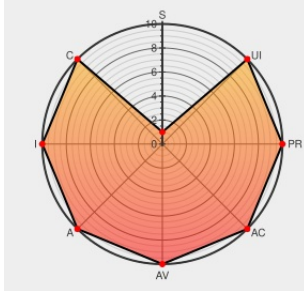
Published on: 04/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:58 PM UTC

CVE-2019-14111

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [lpq6018](#) from [Qualcomm](#) contain the following vulnerability:

Possible buffer overflow while handling NAN reception of NMF in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, Rennell, SC7180, SC8180X, SM6150, SM7150, SM8150, SXR2130

CVE-2019-14111 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 Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking version IPQ6018, IPQ8074, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, Rennell, SC7180, SC8180X, SM6150, SM7150, SM8150, SXR2130

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
April 2020 Bulletin Qualcomm	Vendor Advisory www.qualcomm.com text/html	Q CONFIRM www.qualcomm.com/company/product-security/bulletins/april-2020-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	lpq6018	-	All	All	All
Hardware 	Qualcomm	lpq6018	-	All	All	All
Operating System	Qualcomm	lpq6018 Firmware	-	All	All	All
Operating System	Qualcomm	lpq6018 Firmware	-	All	All	All
Hardware 	Qualcomm	lpq8074	-	All	All	All
Hardware 	Qualcomm	lpq8074	-	All	All	All
Operating System	Qualcomm	lpq8074 Firmware	-	All	All	All
Operating System	Qualcomm	lpq8074 Firmware	-	All	All	All
Hardware 	Qualcomm	Nicobar	-	All	All	All
Hardware 	Qualcomm	Nicobar	-	All	All	All
Operating System	Qualcomm	Nicobar Firmware	-	All	All	All
Operating System	Qualcomm	Nicobar Firmware	-	All	All	All
Hardware 	Qualcomm	Qca6390	-	All	All	All
Hardware 	Qualcomm	Qca6390	-	All	All	All
Operating System	Qualcomm	Qca6390 Firmware	-	All	All	All
Operating System	Qualcomm	Qca6390 Firmware	-	All	All	All
Hardware 	Qualcomm	Qca8081	-	All	All	All

Hardware  	Qualcomm	Qca8081	-	All	All	All
Operating System	Qualcomm	Qca8081 Firmware	-	All	All	All
Operating System	Qualcomm	Qca8081 Firmware	-	All	All	All
Hardware  	Qualcomm	Qcn7605	-	All	All	All
Hardware  	Qualcomm	Qcn7605	-	All	All	All
Operating System	Qualcomm	Qcn7605 Firmware	-	All	All	All
Operating System	Qualcomm	Qcn7605 Firmware	-	All	All	All
Hardware  	Qualcomm	Qcs404	-	All	All	All
Hardware  	Qualcomm	Qcs404	-	All	All	All
Operating System	Qualcomm	Qcs404 Firmware	-	All	All	All
Operating System	Qualcomm	Qcs404 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	Rennell	-	All	All	All
Hardware  	Qualcomm	Rennell	-	All	All	All
Operating System	Qualcomm	Rennell Firmware	-	All	All	All
Operating System	Qualcomm	Rennell Firmware	-	All	All	All
Hardware  	Qualcomm	Sc7180	-	All	All	All
Hardware  	Qualcomm	Sc7180	-	All	All	All
Operating System	Qualcomm	Sc7180 Firmware	-	All	All	All
Operating System	Qualcomm	Sc7180 Firmware	-	All	All	All
Hardware  	Qualcomm	Sc8180x	-	All	All	All
Hardware  	Qualcomm	Sc8180x	-	All	All	All
Operating System	Qualcomm	Sc8180x Firmware	-	All	All	All
Operating System	Qualcomm	Sc8180x Firmware	-	All	All	All

Operating System	Qualcomm	Sm6150 Firmware	-	All	All	All
Hardware	Qualcomm	Sm6150	-	All	All	All
Hardware	Qualcomm	Sm6150	-	All	All	All
Operating System	Qualcomm	Sm6150 Firmware	-	All	All	All
Operating System	Qualcomm	Sm6150 Firmware	-	All	All	All
Hardware	Qualcomm	Sm7150	-	All	All	All
Hardware	Qualcomm	Sm7150	-	All	All	All
Operating System	Qualcomm	Sm7150 Firmware	-	All	All	All
Operating System	Qualcomm	Sm7150 Firmware	-	All	All	All
Hardware	Qualcomm	Sm8150	-	All	All	All
Hardware	Qualcomm	Sm8150	-	All	All	All
Operating System	Qualcomm	Sm8150 Firmware	-	All	All	All
Operating System	Qualcomm	Sm8150 Firmware	-	All	All	All
Hardware	Qualcomm	Sxr2130	-	All	All	All
Hardware	Qualcomm	Sxr2130	-	All	All	All
Operating System	Qualcomm	Sxr2130 Firmware	-	All	All	All
Operating System	Qualcomm	Sxr2130 Firmware	-	All	All	All
cpe:2.3:h:qualcomm:ipq6018:-:~::~:						
cpe:2.3:h:qualcomm:ipq6018:-:~::~:						
cpe:2.3:o:qualcomm:ipq6018_firmware:-:~::~:						
cpe:2.3:o:qualcomm:ipq6018_firmware:-:~::~:						
cpe:2.3:h:qualcomm:ipq8074:-:~::~:						
cpe:2.3:h:qualcomm:ipq8074:-:~::~:						
cpe:2.3:o:qualcomm:ipq8074_firmware:-:~::~:						
cpe:2.3:o:qualcomm:ipq8074_firmware:-:~::~:						
cpe:2.3:h:qualcomm:nicobar:-:~::~:						
cpe:2.3:h:qualcomm:nicobar:-:~::~:						

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

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

cpe:2.3:h:qualcomm:qca6390:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca6390:-:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qca6390_firmware:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca6390_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qca8081:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:qca8081:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qca8081_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:qca8081_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qcn7605:-:*:*:*:*:*:

cpe:2.3:h:qualcomm:qcn7605:-:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:qcn7605_firmware:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qcn7605_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qcs404:-:*:*:*:*:*:*:

```
cpe:2.3:h:qualcomm:gcs404:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcs404_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcs404_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:qcs405:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:gcs405:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcs405_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcs405_firmware:-:*:*:*:*:*:
```

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

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

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

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

```
cpe:2.3:h:qualcomm:sc7180:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sc7180:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sc7180_firmware:-:.*:.*:.*:.*:.*:.*:.*
```

cpe:2.3:o:qualcomm:sc7180_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sc8180x:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sc8180x:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sc8180x_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sc8180x_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sm6150:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sm6150:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sm6150_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sm6150_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sm7150:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sm7150:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sm7150_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sm7150_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sm8150:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sm8150:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sm8150_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sm8150_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sxr2130:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:sxr2130:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sxr2130_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:sxr2130_firmware:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report