



CVE-2020-3667

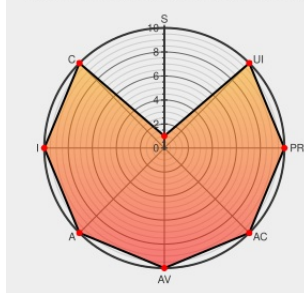
Published on: 09/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3667

[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 [Apq8098](#) from [Qualcomm](#) contain the following vulnerability:

u'Buffer Overflow in mic calculation for WPA due to copying data into buffer without validating the length of buffer' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and

Networking in APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130

CVE-2020-3667 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 IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking version APQ8098, IPQ5018, IPQ6018, IPQ8074, Kamorta, MSM8998, Nicobar, QCA6390, QCA8081, QCS404, QCS405, QCS605, Rennell, SA415M, Saipan, SC7180, SC8180X, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SM8250, SXR1130

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
August 2020 Security Bulletin Qualcomm	Broken Link Vendor Advisory www.qualcomm.com text/html	CONFIRM www.qualcomm.com/company/product-security/bulletins/august-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	Apq8098	-	All	All	All
Hardware 	Qualcomm	Apq8098	-	All	All	All
Operating System	Qualcomm	Apq8098 Firmware	-	All	All	All
Operating System	Qualcomm	Apq8098 Firmware	-	All	All	All
Hardware 	Qualcomm	lpq5018	-	All	All	All
Hardware 	Qualcomm	lpq5018	-	All	All	All
Operating System	Qualcomm	lpq5018 Firmware	-	All	All	All
Operating System	Qualcomm	lpq5018 Firmware	-	All	All	All
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	Ipq8074 Firmware	-	All	All	All
Hardware  	Qualcomm	Kamorta	-	All	All	All
Hardware  	Qualcomm	Kamorta	-	All	All	All
Operating System	Qualcomm	Kamorta Firmware	-	All	All	All
Operating System	Qualcomm	Kamorta Firmware	-	All	All	All
Hardware  	Qualcomm	Msm8998	-	All	All	All
Hardware  	Qualcomm	Msm8998	-	All	All	All
Operating System	Qualcomm	Msm8998 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8998 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	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

Hardware  	Qualcomm	Qcs405	-	All	All	All
Operating System	Qualcomm	Qcs405 Firmware	-	All	All	All
Operating System	Qualcomm	Qcs405 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	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	Sa415m	-	All	All	All
Hardware  	Qualcomm	Sa415m	-	All	All	All
Operating System	Qualcomm	Sa415m Firmware	-	All	All	All
Operating System	Qualcomm	Sa415m Firmware	-	All	All	All
Hardware  	Qualcomm	Saipan	-	All	All	All
Hardware  	Qualcomm	Saipan	-	All	All	All
Operating System	Qualcomm	Saipan Firmware	-	All	All	All
Operating System	Qualcomm	Saipan 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

System						
Hardware  	Qualcomm	Sda845	-	All	All	All
Hardware  	Qualcomm	Sda845	-	All	All	All
Operating System	Qualcomm	Sda845 Firmware	-	All	All	All
Operating System	Qualcomm	Sda845 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	Sdm636	-	All	All	All
Hardware  	Qualcomm	Sdm636	-	All	All	All
Operating System	Qualcomm	Sdm636 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm636 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	Sdm670	-	All	All	All
Hardware  	Qualcomm	Sdm670	-	All	All	All
Operating System	Qualcomm	Sdm670 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm670 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm710	-	All	All	All
Hardware  	Qualcomm	Sdm710	-	All	All	All
Operating System	Qualcomm	Sdm710 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm710 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm845	-	All	All	All
Hardware  	Qualcomm	Sdm845	-	All	All	All
Operating System	Qualcomm	Sdm845 Firmware	-	All	All	All

Երբ.Հ.Յ.Ո.Կալուսումն.արգոսթո.

cpe:2.3:h:qualcomm:apq8098:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:apq8098_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:apq8098_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:ipq5018:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:ipq5018:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:ipq5018_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:ipq5018_firmware:-:*:*:*:*:*:*:
```

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:kamorta:-:*:*:*:*:*:*:

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

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

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

```
cpe:2.3:h:qualcomm:msm8998:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:msm8998:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:msm8998_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:msm8998_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:gca8081:-:*~*~*~*~*~*

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

```
cpe:2.3:o:qualcomm:gca8081_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:gca8081_firmware:-:*:*:*:*:*:*:
```

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

```
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:gcs405:-:*:*:*:*:*:
```

```
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:gcs605:-:*:*:*:*:*:*:

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: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:sa415m:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sa415m:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sa415m firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sa415m_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:saipan:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:saipan:-:*:*:*:*:*:*:

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

```
cpe:2.3:o:qualcomm:saipan_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:sda845:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sda845:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sda845_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sda845_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:sdm636:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm636:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm636_firmware:-:*:*:*:*:*.*
```

```
cpe:2.3:o:qualcomm:sdm636_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:sdm670:-:*:*:*:*:*:
```

```
cpe:2.3:h:qualcomm:sdm670:-:*:*:*:*:*:
```

cpe:2.3:o:qualcomm:sdm670_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm670_firmware:-:*****:
cpe:2.3:h:qualcomm:sdm710:-:*****:
cpe:2.3:h:qualcomm:sdm710:-:*****:
cpe:2.3:o:qualcomm:sdm710_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm710_firmware:-:*****:
cpe:2.3:h:qualcomm:sdm845:-:*****:
cpe:2.3:h:qualcomm:sdm845:-:*****:
cpe:2.3:o:qualcomm:sdm845_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm845_firmware:-:*****:
cpe:2.3:h:qualcomm:sdm850:-:*****:
cpe:2.3:h:qualcomm:sdm850:-:*****:
cpe:2.3:o:qualcomm:sdm850_firmware:-:*****:
cpe:2.3:o:qualcomm:sdm850_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:sm8250:-:*****:
cpe:2.3:h:qualcomm:sm8250:-:*****:

cpe:2.3:o:qualcomm:sm8250_firmware:-:*****:
cpe:2.3:o:qualcomm:sm8250_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 →](#)

© [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](#)