



CVE-2020-3693

Published on: 11/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3693

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

Certain versions of [Apq8009](#) from [Qualcomm](#) contain the following vulnerability:

u'Use out of range pointer issue can occur due to incorrect buffer range check during the execution of qseecom.' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8098,

Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130

CVE-2020-3693 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 IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables version APQ8009, APQ8017, APQ8053, APQ8098, Bitra, MSM8909W, MSM8996AU, Nicobar, QCM2150, QCS605, Saipan, SDM429W, SDX20, SM6150, SM8150, SM8250, SXR2130

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: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
October 2020 Security Bulletin Qualcomm	Patch Vendor Advisory www.qualcomm.com text/html	Q MISC www.qualcomm.com/company/product-security/bulletins/october-2020-security-bulletin
Page not found	Broken Link www.qualcomm.com text/html Inactive Link Not Archived	Q CONFIRM www.qualcomm.com/company/product-security/bulletins/october-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	Apq8009	-	All	All	All
Hardware 	Qualcomm	Apq8009	-	All	All	All
Operating System	Qualcomm	Apq8009 Firmware	-	All	All	All
Operating System	Qualcomm	Apq8009 Firmware	-	All	All	All
Hardware 	Qualcomm	Apq8017	-	All	All	All
Hardware 	Qualcomm	Apq8017	-	All	All	All
Operating System	Qualcomm	Apq8017 Firmware	-	All	All	All
Operating System	Qualcomm	Apq8017 Firmware	-	All	All	All
Hardware 	Qualcomm	Apq8053	-	All	All	All
Hardware 	Qualcomm	Apq8053	-	All	All	All
Operating System	Qualcomm	Apq8053 Firmware	-	All	All	All
Operating System	Qualcomm	Apq8053 Firmware	-	All	All	All
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	Bitra	-	All	All	All
Hardware  	Qualcomm	Bitra	-	All	All	All
Operating System	Qualcomm	Bitra Firmware	-	All	All	All
Operating System	Qualcomm	Bitra Firmware	-	All	All	All
Hardware  	Qualcomm	Msm8909w	-	All	All	All
Hardware  	Qualcomm	Msm8909w	-	All	All	All
Operating System	Qualcomm	Msm8909w Firmware	-	All	All	All
Operating System	Qualcomm	Msm8909w 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	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	Qcm2150	-	All	All	All
Hardware  	Qualcomm	Qcm2150	-	All	All	All
Operating System	Qualcomm	Qcm2150 Firmware	-	All	All	All
Operating System	Qualcomm	Qcm2150 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	Saipan	-	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	Sdm429w	-	All	All	All
Hardware 	Qualcomm	Sdm429w	-	All	All	All
Operating System	Qualcomm	Sdm429w Firmware	-	All	All	All
Operating System	Qualcomm	Sdm429w Firmware	-	All	All	All
Hardware 	Qualcomm	Sdx20	-	All	All	All
Hardware 	Qualcomm	Sdx20	-	All	All	All
Operating System	Qualcomm	Sdx20 Firmware	-	All	All	All
Operating System	Qualcomm	Sdx20 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	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	Sm8250	-	All	All	All
Hardware 	Qualcomm	Sm8250	-	All	All	All
Operating System	Qualcomm	Sm8250 Firmware	-	All	All	All
Operating System	Qualcomm	Sm8250 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:apq8009:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:apq8009:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:apq8009_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:apq8009_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:apq8017:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:apq8017:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:apq8017_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:apq8017_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:apq8053:-:*:*:*:*:*:

cpe:2.3:h:qualcomm:apq8053:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:apq8053_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:apq8053_firmware:-:*:*:*:*:*:*:
```

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

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:bitra:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:bitra:-:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:bitra_firmware:-:*:*:*:*:*:*:

cpe:2.3:o:qualcomm:bitra_firmware:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:msm8909w:-:*:*:*:*:*:

cpe:2.3:h:qualcomm:msm8909w:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:msm8909w_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:msm8909w_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: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:qcm2150:-:~::~~::~~::~~::~~::~::

cpe:2.3:h:qualcomm:qcm2150:-:~::~~::~~::~~::~~::~~::~::

```
cpe:2.3:o:qualcomm:qcm2150_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcm2150 firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:h:qualcomm:gcs605:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qcs605:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:qcs605_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcs605_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:sdm429w:-:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdm429w:-:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm429w_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm429w_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdx20:-:*:*:*:*:*:*:

```
cpe:2.3:h:qualcomm:sdx20:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdx20_firmware:-:*:*:*:*:*:
```

cpe:2.3:o:qualcomm:sdx20_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:-:*:*:*:*:*:
```

ሰላም ለሁሉም፡፡

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: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→

© 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