



CVE-2019-10601

Published on: 12/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:39 PM UTC

CVE-2019-10601

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

Certain versions of [Apq8096au](#) from [Qualcomm](#) contain the following vulnerability:

Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in

APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150

CVE-2019-10601 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 Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking version APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150

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
December 2019 Security Bulletin Qualcomm	Patch Vendor Advisory www.qualcomm.com text/html	CONFIRM www.qualcomm.com/company/product-security/bulletins/december-2019-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	Apq8096au	-	All	All	All
Hardware 	Qualcomm	Apq8096au	-	All	All	All
Operating System	Qualcomm	Apq8096au Firmware	-	All	All	All
Operating System	Qualcomm	Apq8096au Firmware	-	All	All	All
Hardware 	Qualcomm	lpg4019	-	All	All	All
Hardware 	Qualcomm	lpg4019	-	All	All	All
Operating System	Qualcomm	lpg4019 Firmware	-	All	All	All
Operating System	Qualcomm	lpg4019 Firmware	-	All	All	All
Hardware 	Qualcomm	lpg8064	-	All	All	All
Hardware 	Qualcomm	lpg8064	-	All	All	All
Operating System	Qualcomm	lpg8064 Firmware	-	All	All	All
Operating System	Qualcomm	lpg8064 Firmware	-	All	All	All
Hardware 	Qualcomm	lpg8074	-	All	All	All
Hardware 	Qualcomm	lpg8074	-	All	All	All
Operating System	Qualcomm	lpg8074 Firmware	-	All	All	All
Operating System	Qualcomm	lpg8074 Firmware	-	All	All	All
Hardware 	Qualcomm	Msm8996au	-	All	All	All

Hardware 	Qualcomm	Memories	-	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	Qca6574au	-	All	All	All
Hardware 	Qualcomm	Qca6574au	-	All	All	All
Operating System	Qualcomm	Qca6574au Firmware	-	All	All	All
Operating System	Qualcomm	Qca6574au 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	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	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	Sdm845	-	All	All	All
Hardware 🇳🇵 ↗️	Qualcomm	Sdm845	-	All	All	All
Operating System	Qualcomm	Sdm845 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm845 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
cpe:2.3:h:qualcomm:apq8096au:-:*~::~:						
cpe:2.3:h:qualcomm:apq8096au:-:*~::~:						
cpe:2.3:o:qualcomm:apq8096au_firmware:-:*~::~:						
cpe:2.3:o:qualcomm:apq8096au_firmware:-:*~::~:						
cpe:2.3:h:qualcomm:ipq4019:-:*~::~:						
cpe:2.3:h:qualcomm:ipq4019:-:*~::~:						

cpe:2.3:o:qualcomm:ipq4019_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:ipq4019_firmware:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:ipq8064:-:*:*:*:*:*:
cpe:2.3:h:qualcomm:ipq8064:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:ipq8064_firmware:-:*:*:*:*:*:
cpe:2.3:o:qualcomm:ipq8064_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: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:qca6574au:-:*:*:*:*::~
cpe:2.3:h:qualcomm:qca6574au:-:*:*:*:*::~
cpe:2.3:o:qualcomm:qca6574au_firmware:-:*:*:*:*::~
cpe:2.3:o:qualcomm:qca6574au_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:qcs405:-:*:*:*:*::~
cpe:2.3:h:qualcomm:qcs405:-:*:*:*:*::~

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

```
cpe:2.3:o:qualcomm:qcs405_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: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: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:-:*:*:*:*:*:*:

```
opn:2 3: Qualcomm:sm8150_firmware: *.*.*.*.*.*.*.*
```

```
cpe:2.3.0:qualcomm:sm8150_firmware:-.*:*:*:*:*:
```

```
cpe:2.3.0:qualcomm:sm8150_firmware:-.*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

[← Previous ID](#)

Next ID→

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

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