



CVE-2019-2317

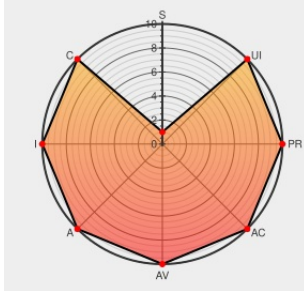
Published on: 03/05/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:04 PM UTC

CVE-2019-2317

[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 [Msm8905](#) from [Qualcomm](#) contain the following vulnerability:

The secret key used to make the Initial Sequence Number in the TCP SYN packet could be brute forced and therefore can be predicted in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8905,

MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, Nicobar, QCM2150, QM215, SC8180X, SDM429, SDM439, SDM450, SDM632, SDX24, SDX55, SM6150, SM7150, SM8150

CVE-2019-2317 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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables** version **MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, Nicobar, QCM2150, QM215, SC8180X, SDM429, SDM439, SDM450, SDM632, SDX24, SDX55, SM6150, SM7150, SM8150**

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: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

March 2020 Security Bulletin | Qualcomm

Vendor Advisory
www.qualcomm.com
text/html

 www.qualcomm.com/company/product-security/bulletins/march-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	Msm8905	-	All	All	All
Hardware 	Qualcomm	Msm8905	-	All	All	All
Operating System	Qualcomm	Msm8905 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8905 Firmware	-	All	All	All
Hardware 	Qualcomm	Msm8909	-	All	All	All
Hardware 	Qualcomm	Msm8909	-	All	All	All
Operating System	Qualcomm	Msm8909 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8909 Firmware	-	All	All	All
Hardware 	Qualcomm	Msm8917	-	All	All	All
Hardware 	Qualcomm	Msm8917	-	All	All	All
Operating System	Qualcomm	Msm8917 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8917 Firmware	-	All	All	All
Hardware 	Qualcomm	Msm8920	-	All	All	All
Hardware 	Qualcomm	Msm8920	-	All	All	All
Operating System	Qualcomm	Msm8920 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8920 Firmware	-	All	All	All

Hardware  	Qualcomm	Msm8937	-	All	All	All
Hardware  	Qualcomm	Msm8937	-	All	All	All
Operating System	Qualcomm	Msm8937 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8937 Firmware	-	All	All	All
Hardware  	Qualcomm	Msm8940	-	All	All	All
Hardware  	Qualcomm	Msm8940	-	All	All	All
Operating System	Qualcomm	Msm8940 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8940 Firmware	-	All	All	All
Hardware  	Qualcomm	Msm8953	-	All	All	All
Hardware  	Qualcomm	Msm8953	-	All	All	All
Operating System	Qualcomm	Msm8953 Firmware	-	All	All	All
Operating System	Qualcomm	Msm8953 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	Qm215	-	All	All	All
Hardware  	Qualcomm	Qm215	-	All	All	All
Operating System	Qualcomm	Qm215 Firmware	-	All	All	All
Operating System	Qualcomm	Qm215 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
Hardware  	Qualcomm	Sdm429	-	All	All	All
Hardware  	Qualcomm	Sdm429	-	All	All	All
Operating System	Qualcomm	Sdm429 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm429 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm439	-	All	All	All
Hardware  	Qualcomm	Sdm439	-	All	All	All
Operating System	Qualcomm	Sdm439 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm439 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm450	-	All	All	All
Hardware  	Qualcomm	Sdm450	-	All	All	All
Operating System	Qualcomm	Sdm450 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm450 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdm632	-	All	All	All
Hardware  	Qualcomm	Sdm632	-	All	All	All
Operating System	Qualcomm	Sdm632 Firmware	-	All	All	All
Operating System	Qualcomm	Sdm632 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdx24	-	All	All	All
Hardware  	Qualcomm	Sdx24	-	All	All	All
Operating System	Qualcomm	Sdx24 Firmware	-	All	All	All
Operating System	Qualcomm	Sdx24 Firmware	-	All	All	All
Hardware  	Qualcomm	Sdx55	-	All	All	All
Hardware  	Qualcomm	Sdx55	-	All	All	All
Operating System	Qualcomm	Sdx55 Firmware	-	All	All	All
Operating System	Qualcomm	Sdx55 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:msm8905:-:~::~:							
cpe:2.3:h:qualcomm:msm8905:-:~::~:							
cpe:2.3:o:qualcomm:msm8905_firmware:-:~::~:							
cpe:2.3:o:qualcomm:msm8905_firmware:-:~::~:							
cpe:2.3:h:qualcomm:msm8909:-:~::~:							
cpe:2.3:h:qualcomm:msm8909:-:~::~:							
cpe:2.3:o:qualcomm:msm8909_firmware:-:~::~:							
cpe:2.3:o:qualcomm:msm8909_firmware:-:~::~:							
cpe:2.3:h:qualcomm:msm8917:-:~::~:							
cpe:2.3:h:qualcomm:msm8917:-:~::~:							
cpe:2.3:o:qualcomm:msm8917_firmware:-:~::~:							
cpe:2.3:o:qualcomm:msm8917_firmware:-:~::~:							
cpe:2.3:h:qualcomm:msm8920:-:~::~:							
cpe:2.3:h:qualcomm:msm8920:-:~::~:							
cpe:2.3:o:qualcomm:msm8920_firmware:-:~::~:							
cpe:2.3:o:qualcomm:msm8920_firmware:-:~::~:							
cpe:2.3:h:qualcomm:msm8937:-:~::~:							

cpe:2.3:h:qualcomm:msm8937:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:msm8937_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:msm8937_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:msm8940:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:msm8940:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:msm8940_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:msm8940_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:msm8953:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:msm8953:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:msm8953_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:msm8953_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:qm215:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:h:qualcomm:qm215:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:qm215_firmware:-:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:qualcomm:qm215_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:sdm429:-:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:qualcomm:sdm429:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm429 firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm429 firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdm439:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdm439:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm439_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm439_firmware:-:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdm450:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdm450:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm450_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdm450_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdm632:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdm632:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdm632 firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:sdm632_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdx24:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdx24:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdx24_firmware:-:*:*:*:*:*:*
```

```
cpe:2.3:o:qualcomm:sdx24_firmware:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:sdx55:-:*:*:*:*:*:*:

cpe:2.3:h:qualcomm:sdx55:-:*:*:*:*:*:*:

```
cpe:2.3:o:qualcomm:sdx55_firmware:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sdx55 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:-:*:*:*:*:*:*:

000-2 2-b-aualcomm-em7150. *. *. *. *. *. *. *. *

cpe:2.3:o: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:-:*:*:*:*:*:

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