



# CVE-2019-14089

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

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

## CVE-2019-14089

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

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

u'Keymaster attestation key and device IDs provisioning which is a one time process is incorrectly allowed to be re-provisioned after a user data erase or a factory reset' in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired

Infrastructure and Networking in Kamorta, Nicobar, QCS404, QCS610, Rennell, SA515M, SA6155P, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130

CVE-2019-14089 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 Wired Infrastructure and Networking version Kamorta, Nicobar, QCS404, QCS610, Rennell, SA515M, SA6155P, SC7180, SC8180X, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130

CVSS3 Score: **7.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.2 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>LOCAL</b>           | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                              | Tags                                                                                             | Link                                                                                                                                                                                            |
|------------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| August 2020 Bulletin                     | <a href="#">Vendor Advisory</a><br><a href="#">www.qualcomm.com</a><br><a href="#">text/html</a> | Q MISC <a href="http://www.qualcomm.com/company/product-security/bulletins/august-2020-security-bulletin">www.qualcomm.com/company/product-security/bulletins/august-2020-security-bulletin</a> |
| August 2020 Security Bulletin   Qualcomm | <a href="#">Broken Link</a><br><a href="#">www.qualcomm.com</a><br><a href="#">text/html</a>     | Q CONFIRM <a href="http://www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin">www.qualcomm.com/company/product-security/bulletins/august-2020-bulletin</a>                |

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](mailto: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   | <a href="#">Qualcomm</a> | <a href="#">Kamorta</a>          | -       | All    | All     | All      |
| Hardware  | <a href="#">Qualcomm</a> | <a href="#">Kamorta</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Qualcomm</a> | <a href="#">Kamorta Firmware</a> | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Qualcomm</a> | <a href="#">Kamorta Firmware</a> | -       | All    | All     | All      |
| Hardware  | <a href="#">Qualcomm</a> | <a href="#">Nicobar</a>          | -       | All    | All     | All      |
| Hardware  | <a href="#">Qualcomm</a> | <a href="#">Nicobar</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Qualcomm</a> | <a href="#">Nicobar Firmware</a> | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Qualcomm</a> | <a href="#">Nicobar Firmware</a> | -       | All    | All     | All      |
| Hardware  | <a href="#">Qualcomm</a> | <a href="#">Qcs404</a>           | -       | All    | All     | All      |
| Hardware  | <a href="#">Qualcomm</a> | <a href="#">Qcs404</a>           | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Qualcomm</a> | <a href="#">Qcs404 Firmware</a>  | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Qualcomm</a> | <a href="#">Qcs404 Firmware</a>  | -       | All    | All     | All      |
| Hardware  | <a href="#">Qualcomm</a> | <a href="#">Qcs610</a>           | -       | All    | All     | All      |
| Hardware  | <a href="#">Qualcomm</a> | <a href="#">Qcs610</a>           | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Qualcomm</a> | <a href="#">Qcs610 Firmware</a>  | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Qualcomm</a> | <a href="#">Qcs610 Firmware</a>  | -       | All    | All     | All      |

| Operating System                                                                                                                                                                 | Qualcomm                 | Secure Firmware                  |   | ... | ... | ... |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------------|---|-----|-----|-----|
| Hardware       | <a href="#">Qualcomm</a> | <a href="#">Rennell</a>          | - | All | All | All |
| Hardware       | <a href="#">Qualcomm</a> | <a href="#">Rennell</a>          | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Rennell Firmware</a> | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Rennell Firmware</a> | - | All | All | All |
| Hardware       | <a href="#">Qualcomm</a> | <a href="#">Sa515m</a>           | - | All | All | All |
| Hardware       | <a href="#">Qualcomm</a> | <a href="#">Sa515m</a>           | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sa515m Firmware</a>  | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sa515m Firmware</a>  | - | All | All | All |
| Hardware       | <a href="#">Qualcomm</a> | <a href="#">Sa6155p</a>          | - | All | All | All |
| Hardware       | <a href="#">Qualcomm</a> | <a href="#">Sa6155p</a>          | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sa6155p Firmware</a> | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sa6155p Firmware</a> | - | All | All | All |
| Hardware   | <a href="#">Qualcomm</a> | <a href="#">Sc7180</a>           | - | All | All | All |
| Hardware   | <a href="#">Qualcomm</a> | <a href="#">Sc7180</a>           | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sc7180 Firmware</a>  | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sc7180 Firmware</a>  | - | All | All | All |
| Hardware   | <a href="#">Qualcomm</a> | <a href="#">Sc8180x</a>          | - | All | All | All |
| Hardware   | <a href="#">Qualcomm</a> | <a href="#">Sc8180x</a>          | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sc8180x Firmware</a> | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sc8180x Firmware</a> | - | All | All | All |
| Hardware   | <a href="#">Qualcomm</a> | <a href="#">Sdx55</a>            | - | All | All | All |
| Hardware   | <a href="#">Qualcomm</a> | <a href="#">Sdx55</a>            | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sdx55 Firmware</a>   | - | All | All | All |
| Operating System                                                                                                                                                                 | <a href="#">Qualcomm</a> | <a href="#">Sdx55 Firmware</a>   | - | All | All | All |
| Hardware   | <a href="#">Qualcomm</a> | <a href="#">Sm6150</a>           | - | All | All | All |
| Hardware   | <a href="#">Qualcomm</a> | <a href="#">Sm6150</a>           | - | 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 | 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: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: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:qcs404:-:*~::~:           |          |                  |   |     |     |     |

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

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

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

```
cpe:2.3:h:qualcomm:qcs610:-:*:*:*:*:*:*:
```

cpe:2.3:h:qualcomm:qcs610:-:\*:\*:\*:\*:\*:\*:

```
cpe:2.3:o:qualcomm:qcs610_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:qcs610_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:sa515m:-:\*:\*:\*:\*:\*:

cpe:2.3:h:qualcomm:sa515m:-:\*:\*:\*:\*:\*:

```
cpe:2.3:o:qualcomm:sa515m_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sa515m firmware:-:*:*:*:*:*:*
```

cpe:2.3:h:qualcomm:sa6155p:-:\*:\*:\*:\*:\*:

cpe:2.3:h:qualcomm:sa6155p:-:\*:\*:\*:\*:\*:

```
cpe:2.3:o:qualcomm:sa6155p_firmware:-:*:*:*:*:*:
```

```
cpe:2.3:o:qualcomm:sa6155p_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: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:-:\*:\*:\*:\*:\*:\*:

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: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→

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](#)