



# CVE-2020-3692

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2020-3692   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | product-security@qualcomm.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2020-11-02 07:15:00 UTC   |
| <b>Updated</b>         | 2020-11-06 16:06:00 UTC   |
| <b>Description</b>     | u'Possible buffer overflow while updating output buffer for IMEI and Gateway Address due to lack of check of input validation |

## Risk And Classification

### Problem Types: CWE-120

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                   | Product                          | Version | Update | Edition | Language |
|------------------|--------------------------|----------------------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Agatti</a>           | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Agatti</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Agatti Firmware</a>  | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Agatti Firmware</a>  | -       | All    | All     | All      |
| 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="#">Qcm6125</a>          | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Qcm6125</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Qcm6125 Firmware</a> | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Qcm6125 Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Qcs610</a>           | -       | All    | All     | All      |

|                  |          |                  |   |     |     |     |
|------------------|----------|------------------|---|-----|-----|-----|
| Hardware         | Qualcomm | Qcs610           | - | All | All | All |
| Operating System | Qualcomm | Qcs610 Firmware  | - | All | All | All |
| Operating System | Qualcomm | Qcs610 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 |
| 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 |
| 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 |

## References

| Reference                                 | Source  | Link   | Tags                |
|---|---------|--|---------------------|
| October 2020 Security Bulletin   Qualcomm | MISC    | <a href="http://www.qualcomm.com">www.qualcomm.com</a> | Vendor Advisory     |
| Page not found                            | CONFIRM | <a href="http://www.qualcomm.com">www.qualcomm.com</a> | Broken Link         |
| CVE Program record                        | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>           | canonical           |
| NVD vulnerability detail                  | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>         | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)