



CVE-2021-35129

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-35129 |
| State | PUBLIC |
| Assigner | product-security@qualcomm.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-06-14 10:15:00 UTC |
| Updated | 2023-04-19 17:10:00 UTC |
| Description | Memory corruption in BT controller due to improper length check while processing vendor specific commands in Snapdragon |

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------|----------------------------------|---------|--------|---------|----------|
| Hardware | Qualcomm | Ar8035 | - | All | All | All |
| Operating System | Qualcomm | Ar8035 Firmware | - | All | All | All |
| Hardware | Qualcomm | Ipq5010 | - | All | All | All |
| Operating System | Qualcomm | Ipq5010 Firmware | - | All | All | All |
| Hardware | Qualcomm | Ipq5018 | - | All | All | All |
| Operating System | Qualcomm | Ipq5018 Firmware | - | All | All | All |
| Hardware | Qualcomm | Ipq5028 | - | All | All | All |
| Operating System | Qualcomm | Ipq5028 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca2062 | - | All | All | All |
| Operating System | Qualcomm | Qca2062 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca2064 | - | All | All | All |
| Operating System | Qualcomm | Qca2064 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca2065 | - | All | All | All |
| Operating System | Qualcomm | Qca2065 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca2066 | - | All | All | All |
| Operating System | Qualcomm | Qca2066 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca6391 | - | All | All | All |

| | | | | | | |
|------------------|----------|------------------|---|-----|-----|-----|
| Operating System | Qualcomm | Qca6391 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca8081 | - | All | All | All |
| Operating System | Qualcomm | Qca8081 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca8337 | - | All | All | All |
| Operating System | Qualcomm | Qca8337 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcc710 | - | All | All | All |
| Operating System | Qualcomm | Qcc710 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcm6490 | - | All | All | All |
| Operating System | Qualcomm | Qcm6490 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn6023 | - | All | All | All |
| Operating System | Qualcomm | Qcn6023 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn6024 | - | All | All | All |
| Operating System | Qualcomm | Qcn6024 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn6100 | - | All | All | All |
| Operating System | Qualcomm | Qcn6100 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn6102 | - | All | All | All |
| Operating System | Qualcomm | Qcn6102 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn6112 | - | All | All | All |
| Operating System | Qualcomm | Qcn6112 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn6122 | - | All | All | All |
| Operating System | Qualcomm | Qcn6122 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn6132 | - | All | All | All |
| Operating System | Qualcomm | Qcn6132 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn9000 | - | All | All | All |
| Operating System | Qualcomm | Qcn9000 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn9012 | - | All | All | All |
| Operating System | Qualcomm | Qcn9012 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn9022 | - | All | All | All |
| Operating System | Qualcomm | Qcn9022 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn9024 | - | All | All | All |
| Operating System | Qualcomm | Qcn9024 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn9070 | - | All | All | All |
| Operating System | Qualcomm | Qcn9070 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn9072 | - | All | All | All |
| Operating System | Qualcomm | Qcn9072 Firmware | - | All | All | All |

| | | | | | | |
|------------------|----------|-----------------------|---|-----|-----|-----|
| Hardware | Qualcomm | Qcn9074 | - | All | All | All |
| Operating System | Qualcomm | Qcn9074 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcn9100 | - | All | All | All |
| Operating System | Qualcomm | Qcn9100 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcs6490 | - | All | All | All |
| Operating System | Qualcomm | Qcs6490 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sd888 | - | All | All | All |
| Hardware | Qualcomm | Sd888 5g | - | All | All | All |
| Operating System | Qualcomm | Sd888 5g Firmware | - | All | All | All |
| Operating System | Qualcomm | Sd888 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sdx65 | - | All | All | All |
| Operating System | Qualcomm | Sdx65 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sd 8cx Gen3 | - | All | All | All |
| Operating System | Qualcomm | Sd 8cx Gen3 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sd 8 Gen1 5g | - | All | All | All |
| Operating System | Qualcomm | Sd 8 Gen1 5g Firmware | - | All | All | All |
| Hardware | Qualcomm | Sm8475 | - | All | All | All |
| Hardware | Qualcomm | Wcd9370 | - | All | All | All |
| Operating System | Qualcomm | Wcd9370 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcd9375 | - | All | All | All |
| Operating System | Qualcomm | Wcd9375 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcd9380 | - | All | All | All |
| Operating System | Qualcomm | Wcd9380 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcd9385 | - | All | All | All |
| Operating System | Qualcomm | Wcd9385 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn6750 | - | All | All | All |
| Operating System | Qualcomm | Wcn6750 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn6850 | - | All | All | All |
| Operating System | Qualcomm | Wcn6850 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn6851 | - | All | All | All |
| Operating System | Qualcomm | Wcn6851 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn6855 | - | All | All | All |
| Operating System | Qualcomm | Wcn6855 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn6856 | - | All | All | All |
| Operating System | Qualcomm | Wcn6856 Firmware | - | All | All | All |

| | | | | | | |
|------------------|----------|------------------|---|-----|-----|-----|
| Hardware | Qualcomm | Wsa8830 | - | All | All | All |
| Operating System | Qualcomm | Wsa8830 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wsa8835 | - | All | All | All |
| Operating System | Qualcomm | Wsa8835 Firmware | - | All | All | All |

References

| Reference | Source | Link | Tags |
|---|---------|--|---------------------|
| April 2022 Security Bulletin Qualcomm | CONFIRM | www.qualcomm.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

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

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