



CVE-2022-33225

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2022-33225 |
| State | PUBLIC |
| Assigner | product-security@qualcomm.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-02-12 04:15:00 UTC |
| Updated | 2023-02-21 18:05:00 UTC |
| Description | Memory corruption due to use after free in trusted application environment. |

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------|------------------------------------|---------|--------|---------|----------|
| Hardware | Qualcomm | Apq8096au | - | All | All | All |
| Operating System | Qualcomm | Apq8096au Firmware | - | All | All | All |
| Hardware | Qualcomm | Mdm9628 | - | All | All | All |
| Operating System | Qualcomm | Mdm9628 Firmware | - | All | All | All |
| Hardware | Qualcomm | Msm8996au | - | All | All | All |
| Operating System | Qualcomm | Msm8996au Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca6390 | - | All | All | All |
| Operating System | Qualcomm | Qca6390 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca6391 | - | All | All | All |
| Operating System | Qualcomm | Qca6391 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca6426 | - | All | All | All |
| Operating System | Qualcomm | Qca6426 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca6436 | - | All | All | All |
| Operating System | Qualcomm | Qca6436 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca6564a | - | All | All | All |
| Hardware | Qualcomm | Qca6564au | - | All | All | All |
| Operating System | Qualcomm | Qca6564au Firmware | - | All | All | All |

| | | | | | | |
|------------------|----------|----------------------|---|-----|-----|-----|
| Operating System | Qualcomm | Qca6564a Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca6574a | - | All | All | All |
| Hardware | Qualcomm | Qca6574au | - | All | All | All |
| Operating System | Qualcomm | Qca6574au Firmware | - | All | All | All |
| Operating System | Qualcomm | Qca6574a Firmware | - | All | All | All |
| Hardware | Qualcomm | Qualcomm215 | - | All | All | All |
| Operating System | Qualcomm | Qualcomm215 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sd205 | - | All | All | All |
| Operating System | Qualcomm | Sd205 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sd210 | - | All | All | All |
| Operating System | Qualcomm | Sd210 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sd429 | - | All | All | All |
| Operating System | Qualcomm | Sd429 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sd865 5g | - | All | All | All |
| Operating System | Qualcomm | Sd865 5g Firmware | - | All | All | All |
| Hardware | Qualcomm | Sd870 | - | All | All | All |
| Operating System | Qualcomm | Sd870 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sdm429w | - | All | All | All |
| Operating System | Qualcomm | Sdm429w Firmware | - | All | All | All |
| Hardware | Qualcomm | Sdx55m | - | All | All | All |
| Operating System | Qualcomm | Sdx55m Firmware | - | All | All | All |
| Hardware | Qualcomm | Sdxr2 5g | - | All | All | All |
| Operating System | Qualcomm | Sdxr2 5g Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcd9340 | - | All | All | All |
| Operating System | Qualcomm | Wcd9340 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcd9380 | - | All | All | All |
| Operating System | Qualcomm | Wcd9380 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn3610 | - | All | All | All |
| Operating System | Qualcomm | Wcn3610 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn3620 | - | All | All | All |
| Operating System | Qualcomm | Wcn3620 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn3660b | - | All | All | All |
| Operating System | Qualcomm | Wcn3660b Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn6850 | - | All | All | All |
| Operating System | Qualcomm | Wcn6850 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wcn6851 | - | All | All | All |

| | | | | | | |
|------------------|----------|------------------|---|-----|-----|-----|
| Hardware | Qualcomm | Wcn6851 | - | All | All | All |
| Operating System | Qualcomm | Wcn6851 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wsa8810 | - | All | All | All |
| Operating System | Qualcomm | Wsa8810 Firmware | - | All | All | All |
| Hardware | Qualcomm | Wsa8815 | - | All | All | All |
| Operating System | Qualcomm | Wsa8815 Firmware | - | All | All | All |

References

| Reference | Source | Link | Tags |
|--------------------------|---------|--|---------------------|
| Qualcomm Documentation | MISC | 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.

Legacy QID Mappings

610465 Google Pixel Android February 2023 Security Patch Missing

© [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](https://mitre.org/licenses).

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