



# CVE-2021-30346

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

## Summary

|                        |                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-30346                                                                                                      |
| <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>       | 2022-06-14 10:15:00 UTC                                                                                             |
| <b>Updated</b>         | 2023-08-08 14:22:00 UTC                                                                                             |
| <b>Description</b>     | RPM secure Stream can access any secure resource due to improper SMMU configuration in Snapdragon Industrial IOT, S |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                   | Product                          | Version | Update | Edition | Language |
|------------------|--------------------------|----------------------------------|---------|--------|---------|----------|
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Ar8035</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Ar8035 Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Qca9984</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Qca9984 Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Qcm2290</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Qcm2290 Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Qcm4290</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Qcm4290 Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Qcs2290</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Qcs2290 Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Qcs405</a>           | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Qcs405 Firmware</a>  | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Qcs4290</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Qcs4290 Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Sd460</a>            | -       | All    | All     | All      |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Sd460 Firmware</a>   | -       | All    | All     | All      |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Sd480</a>            | -       | All    | All     | All      |

|                  |          |                  |   |     |     |     |
|------------------|----------|------------------|---|-----|-----|-----|
| Operating System | Qualcomm | Sd480 Firmware   | - | All | All | All |
| Hardware         | Qualcomm | Sd662            | - | All | All | All |
| Operating System | Qualcomm | Sd662 Firmware   | - | All | All | All |
| Hardware         | Qualcomm | Sd680            | - | All | All | All |
| Operating System | Qualcomm | Sd680 Firmware   | - | All | All | All |
| Hardware         | Qualcomm | Sm6375           | - | All | All | All |
| Operating System | Qualcomm | Sm6375 Firmware  | - | All | All | All |
| Hardware         | Qualcomm | Sw5100           | - | All | All | All |
| Hardware         | Qualcomm | Sw5100p          | - | All | All | All |
| Operating System | Qualcomm | Sw5100p Firmware | - | All | All | All |
| Operating System | Qualcomm | Sw5100 Firmware  | - | 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 | Wcd9385          | - | All | All | All |
| Operating System | Qualcomm | Wcd9385 Firmware | - | All | All | All |
| Hardware         | Qualcomm | Wcn3910          | - | All | All | All |
| Operating System | Qualcomm | Wcn3910 Firmware | - | All | All | All |
| Hardware         | Qualcomm | Wcn3950          | - | All | All | All |
| Operating System | Qualcomm | Wcn3950 Firmware | - | All | All | All |
| Hardware         | Qualcomm | Wcn3980          | - | All | All | All |
| Operating System | Qualcomm | Wcn3980 Firmware | - | All | All | All |
| Hardware         | Qualcomm | Wcn3988          | - | All | All | All |
| Operating System | Qualcomm | Wcn3988 Firmware | - | All | All | All |
| Hardware         | Qualcomm | Wcn3991          | - | All | All | All |
| Operating System | Qualcomm | Wcn3991 Firmware | - | All | All | All |
| Hardware         | Qualcomm | Wcn3998          | - | All | All | All |
| Operating System | Qualcomm | Wcn3998 Firmware | - | All | All | All |
| Hardware         | Qualcomm | Wcn3999          | - | All | All | All |
| Operating System | Qualcomm | Wcn3999 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 |

|                  |                          |                                  |   |     |     |     |
|------------------|--------------------------|----------------------------------|---|-----|-----|-----|
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Wsa8830</a>          | - | All | All | All |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Wsa8830 Firmware</a> | - | All | All | All |
| Hardware         | <a href="#">Qualcomm</a> | <a href="#">Wsa8835</a>          | - | All | All | All |
| Operating System | <a href="#">Qualcomm</a> | <a href="#">Wsa8835 Firmware</a> | - | All | All | All |

## References

| Reference                               | Source  | Link                                                   | Tags                |
|-----------------------------------------|---------|--------------------------------------------------------|---------------------|
| April 2022 Security Bulletin   Qualcomm | CONFIRM | <a href="http://www.qualcomm.com">www.qualcomm.com</a> |                     |
| 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.

## Legacy QID Mappings

[610407](#) Google Android Devices April 2022 Security Patch Missing

© [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](#) 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](#)