# CVE-2019-14134

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2019-14134 |
| **State** | PUBLIC |
| **Assigner** | product-security@qualcomm.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-04-16 11:15:00 UTC |
| **Updated** | 2020-04-21 19:06:00 UTC |
| **Description** | Possible out of bound access in WLAN handler when the received value of length in rx path is shorter than the expected va |

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Qualcomm | Ipq8074 | - | All | All | All |
| Hardware | Qualcomm | Ipq8074 | - | All | All | All |
| Operating System | Qualcomm | Ipq8074 Firmware | - | All | All | All |
| Operating System | Qualcomm | Ipq8074 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qca8081 | - | All | All | All |
| Hardware | Qualcomm | Qca8081 | - | All | All | All |
| Operating System | Qualcomm | Qca8081 Firmware | - | All | All | All |
| Operating System | Qualcomm | Qca8081 Firmware | - | All | All | All |
| Hardware | Qualcomm | Qcs605 | - | All | All | All |
| Hardware | Qualcomm | Qcs605 | - | All | All | All |
| Operating System | Qualcomm | Qcs605 Firmware | - | All | All | All |
| Operating System | Qualcomm | Qcs605 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sda845 | - | All | All | All |
| Hardware | Qualcomm | Sda845 | - | All | All | All |
| Operating System | Qualcomm | Sda845 Firmware | - | All | All | All |
| Operating System | Qualcomm | Sda845 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sdm670 | - | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Hardware | Qualcomm | Sdm670 | - | All | All | All |
| Operating System | Qualcomm | Sdm670 Firmware | - | All | All | All |
| Operating System | Qualcomm | Sdm670 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sdm710 | - | All | All | All |
| Hardware | Qualcomm | Sdm710 | - | All | All | All |
| Operating System | Qualcomm | Sdm710 Firmware | - | All | All | All |
| Operating System | Qualcomm | Sdm710 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sdm845 | - | All | All | All |
| Hardware | Qualcomm | Sdm845 | - | All | All | All |
| Operating System | Qualcomm | Sdm845 Firmware | - | All | All | All |
| Operating System | Qualcomm | Sdm845 Firmware | - | All | All | All |
| Hardware | Qualcomm | Sdm850 | - | All | All | All |
| Hardware | Qualcomm | Sdm850 | - | All | All | All |
| Operating System | Qualcomm | Sdm850 Firmware | - | All | All | All |
| Operating System | Qualcomm | Sdm850 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 | Sxr1130 | - | All | All | All |
| Hardware | Qualcomm | Sxr1130 | - | All | All | All |
| Operating System | Qualcomm | Sxr1130 Firmware | - | All | All | All |
| Operating System | Qualcomm | Sxr1130 Firmware | - | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| April 2020 Bulletin \| Qualcomm | CONFIRM | www.qualcomm.com | Vendor Advisory |

| | | | |
|---|---|---|---|
| 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.