Product Security Advisory: EM919x and EM929x Security Advisory

Sierra Wireless Advisory: SWI-PSA-2024-001

Date: 22 February 2024

Summary

Sierra Wireless – A Semtech Company was recently informed of three vulnerabilities affecting a wide range of Qualcomm chipsets, including those used in the Sierra Wireless EM919x and EM929x cellular modules. These vulnerabilities, published by researchers as part of the 5Ghoul disclosure, were announced as part of Qualcomm's December QTI Security Bulletin.

CVE ID	Description	CVSSv3.1
CVE-2023-33042	Improper input validation leading to a Denial of Service condition. Processing of *RRC Setup Message Handler* incorrectly fails to release or incorrectly releases resources.	7.5 - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2023-33043	Transient Denial of Service (reachable assert) in Modem when a Beam switch request is made with a non-configured BWP (Bandwidth Part).	7.3 - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2023-33044	Transient Denial of Service (reachable assert) condition in Data component of modem while handling TLB control messages received from the network.	7.5 - AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Vulnerability Details

The report which disclosed the vulnerabilities provides additional contextual background to aid companies in understanding the potential exploitation vectors and in gauging their risk profile. The researcher's comments on the three CVEs which impact Sierra Wireless modules include:

- CVE-2023-33042: An attacker within Qualcomm X55/X60 UE radio range can deny or downgrade 5G connectivity by sending a single malformed packet. The user needs to manually reboot the phone to recover 5G connectivity.

- CVE-2023-33043: An attacker within X55/X60 modem-based UE radio range can block 3GPP Modem connectivity by continuously sending an invalid packet.

- CVE-2023-33044: An attacker within X55/X60 UE radio range can block 3GPP Modem connectivity by continuously sending an invalid packet.

These statements are taken from the researcher's disclosure at: https://asset-group.github.io/disclosures/5ghoul/

These statements have not been independently verified by Sierra Wireless.

Affected Products

These vulnerabilities affect all EM9190. EM9191, EM9291, and EM9293 modules and devices using those modules due to their use of the affected Qualcomm chipset.

Recommended Actions

For EM929x modules, Sierra Wireless recommends that customers upgrade to the EM929x Release 2 (SWIX65C_02.15.01.00) firmware version or newer to ensure all three vulnerabilities are addressed.

For EM919x modules, Sierra Wireless recommends that customers upgrade to the EM919x Release 6 (SWIX55C_03.14.10.00) firmware version or newer to address CVE-2023-33044 and CVE-2023-33042. Remediation of CVE-2023-33043 is planned for the upcoming EM919x Release 7 firmware, pending availability of remediation measures from the chipset vendor.

At this time, no mitigations have been provided by Qualcomm.

Credit

Qualcomm has credited Matheus E. Garbelini, Zewen Shang, Sudipta Chattopadhyay, Sumei Sun, and Ernest Kurniawan of the Singapore University of Technology and Design, and I2R, A*STAR. We encourage anyone with a security concern related to Sierra Wireless products to please contact us at security@sierrawireless.com.

Support Contact Information

Sierra Wireless Technical Support is available by phone or web portal from 6:00 to 17:00 PST, Monday to Friday.

Phone (Toll-Free): 1-877-687-7795
Web: https://www.sierrawireless.com/support/community-portal/

Security Bulletins

To see the latest security updates from Sierra Wireless, please visit:
https://www.sierrawireless.com/company/security/