Multiple High Severity Vulnerabilities in Qualcomm and MediaTek Products

MediaTek and Qualcomm have released updates addressing multiple high severity implementation-level 5G vulnerabilities in their products. These vulnerabilities are collectively named the 5Ghoul vulnerabilities by security researchers who discovered them.

To exploit these vulnerabilities, an attacker is not required to obtain any information from the end-user devices as these vulnerabilities can be successfully exploited before any Network Access Server (NAS) authentication is completed. Successful exploitation of the vulnerabilities could allow the attacker to downgrade 5G connectivity and disrupt services temporarily.

A summary of the vulnerabilities can be found in the table below:

CVE Number	**Description**	**Affected Chipsets**
CVE-2023-33042	An improper input validation vulnerability in Qualcomm modem that could allow an attacker to perform denial-of-service (DoS) or 5G connectivity downgrade by sending a malformed Radio Resource Control (RRC) frame.	Qualcomm 3155GIoTModem Qualcomm AR8035 Qualcomm FastConnect6200 Qualcomm FastConnect6700 Qualcomm FastConnect6800 Qualcomm FastConnect6900 Qualcomm FastConnect7800 Qualcomm QCA6391 Qualcomm QCA6421 Qualcomm QCA6426 Qualcomm QCA6431 Qualcomm QCA6436 Qualcomm QCA6574A Qualcomm QCA6595AU Qualcomm QCA6696 Qualcomm QCA6698AQ Qualcomm QCA8081 Qualcomm QCA8337 Qualcomm QCM6490 Qualcomm QCN6024 Qualcomm QCN9024 Qualcomm QCS6490 Qualcomm QCS8550 Qualcomm VideoCollaborationVC3Platform Qualcomm SD855 Qualcomm SD8655G Qualcomm SD888 Qualcomm SDX55 Qualcomm SDX57M Qualcomm SM7250P Qualcomm SM7315 Qualcomm SM7325P Qualcomm Snapdragon4Gen1MobilePlatform Qualcomm Snapdragon4805GMobilePlatform

		Qualcomm Snapdragon480+5GMobilePlatform(SM4350-AC) Qualcomm Snapdragon6905GMobilePlatform Qualcomm Snapdragon6955GMobilePlatform Qualcomm Snapdragon750G5GMobilePlatform Qualcomm Snapdragon7655GMobilePlatform(SM7250-AA) Qualcomm Snapdragon765G5GMobilePlatform(SM7250-AB) Qualcomm Snapdragon768G5GMobilePlatform(SM7250-AC) Qualcomm Snapdragon778G5GMobilePlatform Qualcomm Snapdragon778G+5GMobilePlatform(SM7325-AE) Qualcomm Snapdragon780G5GMobilePlatform Qualcomm Snapdragon782GMobilePlatform(SM7325-AF) Qualcomm Snapdragon7c+Gen3Compute Qualcomm Snapdragon8Gen1MobilePlatform Qualcomm Snapdragon8+Gen1MobilePlatform Qualcomm Snapdragon855MobilePlatform Qualcomm Snapdragon855+/860MobilePlatform(SM8150-AC) Qualcomm Snapdragon8655GMobilePlatform Qualcomm Snapdragon865+5GMobilePlatform(SM8250-AB) Qualcomm Snapdragon8705GMobilePlatform(SM8250-AC) Qualcomm Snapdragon8885GMobilePlatform Qualcomm Snapdragon888+5GMobilePlatform(SM8350-AC) Qualcomm SnapdragonAuto5GModem-RF Qualcomm SnapdragonX555GModem-RFSystem Qualcomm SnapdragonX655GModem-RFSystem Qualcomm SnapdragonX70Modem-RFSystem Qualcomm SnapdragonXR25GPlatform Qualcomm SXR2130

		Qualcomm WCD9341 Qualcomm WCD9360 Qualcomm WCD9370 Qualcomm WCD9375 Qualcomm WCD9380 Qualcomm WCD9385 Qualcomm WCN3988 Qualcomm WCN6740 Qualcomm WSA8810 Qualcomm WSA8815 Qualcomm WSA8830 Qualcomm WSA8835
CVE-2023-33043	A reachable assertion vulnerability in Qualcomm modem that could allow an attacker to perform denial-of-service (DoS) by sending an unconfigured Bandwidth Part (BWP).	Qualcomm AR8035 Qualcomm FastConnect6200 Qualcomm FastConnect6700 Qualcomm FastConnect6900 Qualcomm FastConnect7800 Qualcomm QCA6391 Qualcomm QCA8081 Qualcomm QCA8337 Qualcomm QCM4490 Qualcomm QCM6490 Qualcomm QCM8550 Qualcomm QCN6024 Qualcomm QCN9024 Qualcomm QCS4490 Qualcomm QCS6490 Qualcomm QCS8550 Qualcomm VideoCollaborationVC3Platform Qualcomm SD888 Qualcomm SDX57M Qualcomm SM7315 Qualcomm SM7325P Qualcomm SM8550P Qualcomm Snapdragon4Gen1MobilePlatform Qualcomm Snapdragon4Gen2MobilePlatform Qualcomm Snapdragon4805GMobilePlatform Qualcomm Snapdragon480+5GMobilePlatform(SM4350-AC) Qualcomm Snapdragon6955GMobilePlatform Qualcomm Snapdragon778G5GMobilePlatform Qualcomm Snapdragon778G+5GMobilePlatform(SM7325-AE) Qualcomm Snapdragon780G5GMobilePlatform Qualcomm Snapdragon782GMobilePlatform(SM7325-AF) Qualcomm Snapdragon7c+Gen3Compute

		Qualcomm Snapdragon8Gen1MobilePlatform Qualcomm Snapdragon8Gen2MobilePlatform Qualcomm Snapdragon8+Gen1MobilePlatform Qualcomm Snapdragon8+Gen2MobilePlatform Qualcomm Snapdragon8885GMobilePlatform Qualcomm Snapdragon888+5GMobilePlatform(SM8350-AC) Qualcomm SnapdragonX655GModem-RFSystem Qualcomm SnapdragonX70Modem-RFSystem Qualcomm WCD9370 Qualcomm WCD9375 Qualcomm WCD9380 Qualcomm WCD9385 Qualcomm WCD9390 Qualcomm WCD9395 Qualcomm WCN3950 Qualcomm WCN3988 Qualcomm WCN6740 Qualcomm WSA8810 Qualcomm WSA8815 Qualcomm WSA8830 Qualcomm WSA8832 Qualcomm WSA8835 Qualcomm WSA8840 Qualcomm WSA8845 Qualcomm WSA8845H
CVE-2023-33044	A reachable assertion vulnerability in Qualcomm modem that could allow an attacker to perform denial-of-service (DoS) by sending an invalid NAS packet.	Qualcomm 3155GIoTModem Qualcomm AR8035 Qualcomm FastConnect6200 Qualcomm FastConnect6700 Qualcomm FastConnect6800 Qualcomm FastConnect6900 Qualcomm FastConnect7800 Qualcomm QCA6391 Qualcomm QCA6421 Qualcomm QCA6426 Qualcomm QCA6431 Qualcomm QCA6436 Qualcomm QCA6574A Qualcomm QCA6574AU Qualcomm QCA6595AU Qualcomm QCA6696 Qualcomm QCA6698AQ Qualcomm QCA8081 Qualcomm QCA8337 Qualcomm QCM4490 Qualcomm QCM6490 Qualcomm QCM8550 Qualcomm QCN6024

		Qualcomm QCN9024 Qualcomm QCS4490 Qualcomm QCS6490 Qualcomm QCS8550 Qualcomm Qualcomm®VideoCollaborationVC3Platform Qualcomm SD855 Qualcomm SD8655G Qualcomm SD888 Qualcomm SDX55 Qualcomm SDX57M Qualcomm SM7250P Qualcomm SM7315 Qualcomm SM7325P Qualcomm SM8550P Qualcomm Snapdragon4Gen1MobilePlatform Qualcomm Snapdragon4Gen2MobilePlatform Qualcomm Snapdragon4805GMobilePlatform Qualcomm Snapdragon480+5GMobilePlatform(SM4350-AC) Qualcomm Snapdragon6905GMobilePlatform Qualcomm Snapdragon6955GMobilePlatform Qualcomm Snapdragon750G5GMobilePlatform Qualcomm Snapdragon7655GMobilePlatform(SM7250-AA) Qualcomm Snapdragon765G5GMobilePlatform(SM7250-AB) Qualcomm Snapdragon768G5GMobilePlatform(SM7250-AC) Qualcomm Snapdragon778G5GMobilePlatform Qualcomm Snapdragon778G+5GMobilePlatform(SM7325-AE) Qualcomm Snapdragon780G5GMobilePlatform Qualcomm Snapdragon782GMobilePlatform(SM7325-AF) Qualcomm Snapdragon7c+Gen3Compute Qualcomm Snapdragon8Gen1MobilePlatform Qualcomm Snapdragon8Gen2MobilePlatform Qualcomm Snapdragon8+Gen1MobilePlatform Qualcomm Snapdragon8+Gen2MobilePlatform Qualcomm Snapdragon855MobilePlatform

		Qualcomm Snapdragon855+/860MobilePlatform(SM8150-AC) Qualcomm Snapdragon8655GMobilePlatform Qualcomm Snapdragon865+5GMobilePlatform(SM8250-AB) Qualcomm Snapdragon8705GMobilePlatform(SM8250-AC) Qualcomm Snapdragon8885GMobilePlatform Qualcomm Snapdragon888+5GMobilePlatform(SM8350-AC) Qualcomm SnapdragonAuto5GModem-RF Qualcomm SnapdragonX555GModem-RFSystem Qualcomm SnapdragonX655GModem-RFSystem Qualcomm SnapdragonX70Modem-RFSystem Qualcomm SnapdragonXR25GPlatform Qualcomm SXR2130 Qualcomm WCD9341 Qualcomm WCD9360 Qualcomm WCD9370 Qualcomm WCD9375 Qualcomm WCD9380 Qualcomm WCD9385 Qualcomm WCD9390 Qualcomm WCD9395 Qualcomm WCN3950 Qualcomm WCN3988 Qualcomm WCN6740 Qualcomm WSA8810 Qualcomm WSA8815 Qualcomm WSA8830 Qualcomm WSA8832 Qualcomm WSA8835 Qualcomm WSA8840 Qualcomm WSA8845 Qualcomm WSA8845H
CVE-2023-20702	An invalid memory access vulnerability in MediaTek modem that could allow an attacker to perform denial-of-service (DoS) by sending a malformed Radio Link Control (RLC) header.	MediaTek NR15 MediaTek NR16 MediaTek NR17 MediaTek MT6835 MediaTek MT6873 MediaTek MT6875 MediaTek MT6879 MediaTek MT6883 MediaTek MT6885 MediaTek MT6886

		MediaTek MT6889 MediaTek MT6895 MediaTek MT6980 MediaTek MT6983 MediaTek MT6985 MediaTek MT6990 MediaTek MT8673 MediaTek MT8675 MediaTek MT8791 MediaTek MT8791T MediaTek MT8797 MediaTek MT8798
CVE-2023-32841 CVE-2023-32842 CVE-2023-32843 CVE-2023-32844 CVE-2023-32845 CVE-2023-32846	A reachable assertion vulnerability in MediaTek modem that could allow an attacker to perform denial-of-service (DoS) by sending malformed Radio Resource Control (RRC) messages.	MediaTek NR15 MediaTek NR16 MediaTek NR17 MediaTek MT2735 MediaTek MT2737 MediaTek MT6297 MediaTek MT6298 MediaTek MT6813 MediaTek MT6815 MediaTek MT6833 MediaTek MT6835 MediaTek MT6853 MediaTek MT6855 MediaTek MT6873 MediaTek MT6875 MediaTek MT6875T MediaTek MT6877 MediaTek MT6879 MediaTek MT6880 MediaTek MT6883 MediaTek MT6885 MediaTek MT6886 MediaTek MT6889 MediaTek MT6890 MediaTek MT6891 MediaTek MT6893 MediaTek MT6895 MediaTek MT6895T MediaTek MT6896 MediaTek MT6897 MediaTek MT6980 MediaTek MT6980D MediaTek MT6983 MediaTek MT6985 MediaTek MT6989 MediaTek MT6990

Users and administrators of the affected products are advised to update to the latest versions immediately or as and when they are released.

More information is available here:
https://corp.mediatek.com/product-security-bulletin/November-2023
https://corp.mediatek.com/product-security-bulletin/December-2023
https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2023-bulletin.html
https://www.bleepingcomputer.com/news/security/new-5ghoul-attack-impacts-5g-phones-with-qualcomm-mediatek-chips/
https://asset-group.github.io/disclosures/5ghoul/disclosure.html#x1-210007.6