

New 5Ghoul attack impact 5G Commercial Products with Qualcomm, MediaTek chip

Original report published on: December 07, 2023^[1]

Executive Summary

5Ghoul consists of 14 vulnerabilities discovered by Singapore University of Technology and Design (SUTD) researchers affecting 5G mobile network modems from Qualcomm and MediaTek, and successful exploit leads to downgrade or denial-of-service (DoS) attacks.

Background

10 disclosed vulnerabilities affecting modem firmware implementation^[1] and can be easily exploited over-the-air. The attacker only needs to impersonate the legitimate base station (gNB) by copying its Cell Tower connection parameters (e.g, SSB ARFCN, Tracking Area Code, Physical Cell ID, Point A Frequency), which can be easily accomplished using freely available applications like Cellular-Pro. They do not need details of the target user equipment, such as SIM card details, to complete the Non-Access Stratum^[2] network registration.

If the Received Signal Strength Indicator (RSSI) of the attacker gNB is higher than the legitimate gNB, the target user equipment will connect to the attacker gNB. Once connected, the attacker can exploit the vulnerabilities to launch downgrade or denial-of-service (DoS) attacks.

The 4 remaining vulnerabilities were not publicly published.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE FiGHT techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory:
 - Create, test, and validate detection rules against the threat behaviours.
 - Validate and deny/disable processes, ports and protocols that have no business need.
- Qualcomm and MediaTek have released security bulletins for the disclosed 5Ghoul vulnerabilities and updates were made available to device vendors.^{[3][4]}
- Work with your vendor(s) to identify affected products in your environment and apply the latest security updates or compensating measures.





IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

MITRE FiGHT Tactics and Techniques (<https://fight.mitre.org>)

| Tactic | Technique ID | Technique Name |
|----------------------|-------------------------|--------------------|
| Resource Development | FGT1608 | Stage Capabilities |

| | | |
|--------|-----------------------------|--|
| Impact | FGT1565.002 | Data Manipulation: Transmitted Data Manipulation |
| Impact | FGT1498 | Network Denial of Service |

References

1. ^ "5Ghoul: Unleashing Chaos on 5G Edge Devices"  .
2. ^ "Non-Access Stratum (NAS) Protocol is a functional layer in the NR, LTE, UMTS and GSM wireless telecom protocol stacks between the core network and user equipment"  .
3. ^ "Qualcomm: December 2023 Security Bulletin"  .
4. ^ "MediaTek December 2023 Product Security Bulletin"  .