مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

# Security Updates - MediaTek Chipsets

Tracking #:432317663

Date:02-09-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that MediaTek has released security updates to address multiple vulnerabilities in its products.

## TECHNICAL DETAILS:

MediaTek has released its September 2025 security updates to address multiple vulnerabilities in its modem and system components across various chipset models. These vulnerabilities could allow remote or local privilege escalation, as well as denial-of-service (DoS) attacks.

**High-Severity Vulnerabilities:**

- **CVE-2025-20708** – An out-of-bounds write in the modem subsystem (CWE-787) could allow remote privilege escalation without user interaction when a device connects to a rogue base station. Affects over 70 chipset models, including MT6853, MT6877, MT6899, MT6980, and MT8893, running modem firmware NR15 through NR17R.
- **CVE-2025-20703** – An out-of-bounds read in the modem subsystem (CWE-125) that could cause remote denial of service under similar conditions, affecting the same chipsets and firmware versions.
- **CVE-2025-20704** – A second out-of-bounds write (CWE-787) in modem firmware NR17/NR17R allows remote privilege escalation with user interaction. Impacts a narrower subset of chipsets such as MT6835T, MT6878M, and MT8883.

**Medium-Severity Vulnerabilities:**

- **CVE-2025-20705** – Use-after-free in the **monitor_hang** driver (CWE-416) may permit local privilege escalation on devices where an attacker already has System privileges. Affected platforms include Android 13.0–16.0, OpenWRT 19.07/21.02, and Yocto 2.6. Chipsets include MT6765, MT6789, MT8169, and others.
- **CVE-2025-20706** – Use-after-free in the **mbrain** component, impacting Android 14.0–15.0 on chipsets such as MT6989 and MT8678, potentially allowing local escalation.
- **CVE-2025-20707** – Use-after-free in the **geniezone** module, affecting Android 13.0–15.0 on chipsets including MT6853, MT8792, and MT8883, with similar local privilege escalation risk.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to ensure all devices using affected MediaTek chipsets are updated with the latest security patches provided by OEMs or software vendors

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://corp.mediatek.com/product-security-bulletin/September-2025