مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- MediaTek Chipsets

Tracking #:432317048

Date:08-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed MediaTek has disclosed multiple security vulnerabilities affecting its chipsets used in smartphones, tablets, AIoT devices, smart displays, OTT platforms, computer vision systems, audio devices, and TVs.

TECHNICAL DETAILS:

MediaTek has disclosed multiple security vulnerabilities affecting its chipsets used in smartphones, tablets, AIoT devices, smart displays, OTT platforms, computer vision systems, audio devices, and TVs. Among the issues, one has been rated Critical (CVE-2025-20654), which allows unauthenticated Remote Code Execution (RCE) through an out-of-bounds write in the WLAN service. Four vulnerabilities are rated High, leading to local privilege escalation (EoP) or information disclosure, and six are classified as Medium severity, which include denial of service, information disclosure, and local EoP vectors.

Vulnerability Details:

CVE	Title	Severity	Impact
CVE-2025-20654	Out-of-bounds write in WLAN	Critical	Remote Code Execution without user interaction. Impacts MT6890, MT7622, MT7915, MT7916, MT7981, MT7986. Affected SDKs: ≤7.4.0.1 / 7.6.7.0 / OpenWrt 19.07 & 21.02
CVE-2025-20655	Out-of-bounds read in Keymaster	High	Local disclosure requiring System privilege. MT9972, Android 12/14
CVE-2025-20656	Out-of-bounds write in DA	High	Local privilege escalation with physical access. Multiple chipsets, Android 12–15, OpenWRT, Yocto, RDK-B
CVE-2025-20657	Out-of-bounds write in VDEC	High	Local EoP via permission bypass. Android 12/15
CVE-2025-20658	Out-of-bounds write in DA	High	Local EoP through logic error. Android 12–15
CVE-2025-20659	Out-of-bounds read in Modem	Medium	Remote DoS via rogue base station. Impacts a vast range of MediaTek SoCs
CVE-2025-20660 to 20662	Out-of-bounds read in DRMServer (PlayReady TA)	Medium	Local privilege escalation requiring System privilege. MT9972
CVE-2025-20663 & 20664	Uncaught exception in WLAN	Medium	Remote (adjacent) info disclosure. SDK 7.4.0.1–8.2.1.4

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/April-2025#CVE_2025_20655