مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Security Vulnerabilities in MediaTek Chipsets

Tracking #:432316820

Date:04-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed MediaTek has released its February 2025 Product Security Bulletin, highlighting multiple critical vulnerabilities in its chipsets used in smartphones, tablets, and other devices.

TECHNICAL DETAILS:

MediaTek has released its February 2025 Product Security Bulletin, highlighting multiple critical vulnerabilities in its chipsets used in smartphones, tablets, and other devices.

These vulnerabilities, some of which can lead to remote code execution, privilege escalation, and denial of service, affect various MediaTek chipsets, including the MT7603, MT7615, MT7622, and MT7915. Specifically, vulnerabilities in the WLAN AP driver (CVE-2025-20633, CVE-2025-20632, CVE-2025-20631) and the modem (CVE-2025-20630) pose serious security risks.

Vulnerability Overview:

1. WLAN AP Driver Vulnerabilities:
   - CVE-2025-20633, CVE-2025-20632, CVE-2025-20631
   - Severity: Critical
   - Description: A set of vulnerabilities in the WLAN AP driver could allow remote attackers to execute arbitrary code on affected devices without requiring user interaction or elevated privileges. The vulnerabilities arise from improper bounds checking in the WLAN AP driver. These flaws are particularly concerning because they could be exploited remotely, potentially compromising the device without any local access.
   - Affected Chipsets: MT7603, MT7615, MT7622, MT7915 running SDK release 7.4.0.1 and earlier.

2. Modem Vulnerability:
   - CVE-2025-20630
   - Severity: High
   - Description: This vulnerability involves potential out-of-bounds writes in the modem. Exploiting this flaw could lead to remote code execution or local privilege escalation, allowing attackers to execute arbitrary code with elevated privileges. This could affect the integrity and security of the device's communications.
   - Affected Chipsets: Various MediaTek chipsets and software versions.

Other Driver Vulnerabilities:
Several high-severity vulnerabilities have been identified in various drivers within MediaTek chipsets. These could lead to remote code execution or local privilege escalation, depending on the specific nature of the vulnerability and the device configuration.

RECOMMENDATIONS:

- Patch Availability: MediaTek and device manufacturers are actively releasing firmware and software patches for the affected chipsets and devices. Users are strongly encouraged to check for updates from their respective OEMs and install them immediately to protect their devices.

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/February-2025