February 2025 Product Security Bulletin

Published 2025-02-03

The MediaTek Product Security Bulletin contains details of security vulnerabilities affecting MediaTek Smartphone, Tablet, AIoT, Smart display, Smart platform, OTT, Computer Vision, Audio, and TV chipsets. Device OEMs have been notified of all the issues and the corresponding security patches for at least two months before publication.

The severity of the identified vulnerabilities was conducted based on the Common Vulnerability Scoring System version 3.1 (CVSS v3.1).

Summary

Severity	CVEs

Medium	CVE-2025-20638, CVE-2025-20639, CVE-2025-20640, CVE-2025-20641, CVE-2025-20642, CVE-2025-20643, CVE-2024-20147

Details

CVE	**CVE-2025-20633**
Title	Out-of-bounds write in wlan
Severity	High
Vulnerability Type	RCE
CWE	CWE-787 Out-of-bounds Write
Description	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.
Affected Chipsets	MT7603, MT7615, MT7622, MT7915
Affected Software Versions	SDK release 7.4.0.1 and before
Report Source	External

CVE	**CVE-2025-20632**
Title	Out-of-bounds write in wlan

Description	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
Affected Chipsets	MT7615, MT7622, MT7663, MT7915, MT7916, MT7981, MT7986
Affected Software Versions	SDK release 7.6.7.2 and before
Report Source	External

CVE	**CVE-2025-20631**
Title	Out-of-bounds write in wlan
Severity	High
Vulnerability Type	EoP
CWE	CWE-787 Out-of-bounds Write
Description	In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
Affected Chipsets	MT7615, MT7622, MT7663, MT7915, MT7916, MT7981, MT7986

CVE	**CVE-2025-20634**
Title	Out-of-bounds write in Modem
Severity	High
Vulnerability Type	RCE
CWE	CWE-787 Out-of-bounds Write
Description	In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation.
Affected Chipsets	MT2737, MT6813, MT6835, MT6835T, MT6878, MT6878M, MT6879, MT6886, MT6895, MT6895TT, MT6896, MT6897, MT6899, MT6980, MT6980D, MT6983, MT6983T, MT6985, MT6985T, MT6989, MT6989T, MT6990, MT6991, MT8673, MT8676, MT8678, MT8795T, MT8798, MT8863
Affected Software Versions	Modem NR16, NR17, NR17R
Report Source	Internal

CVE	**CVE-2025-20635**
Title	Out-of-bounds write in DA
Severity	High

	bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation.
Affected Chipsets	MT2737, MT6781, MT6789, MT6835, MT6855, MT6878, MT6879, MT6880, MT6886, MT6890, MT6895, MT6897, MT6980, MT6983, MT6985, MT6989, MT6990, MT8370, MT8390
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0 / openWRT 19.07, 21.02, 23.05 / Yocto 4.0 / RDK-B 22Q3, 24Q1
Report Source	Internal

CVE	**CVE-2025-20636**
Title	Out-of-bounds write in secmem
Severity	High
Vulnerability Type	EoP
CWE	CWE-787 Out-of-bounds Write
Description	In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation.

	MT6893, MT6895, MT6983, MT6985, MT8321, MT8385, MT8666, MT8667, MT8673, MT8755, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8796, MT8797, MT8798
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2025-20637**
Title	Uncaught exception in network
Severity	High
Vulnerability Type	DoS
CWE	CWE-248 Uncaught Exception
Description	In network HW, there is a possible system hang due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.
Affected Chipsets	MT7981, MT7986
Affected Software Versions	SDK release 7.6.7.0 and before
Report Source	Internal

CVE	**CVE-2024-20141**

CWE	CWE-123 Write-what-where Condition
Description	In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6771, MT6779, MT6781, MT6785, MT6833, MT6853, MT6873, MT6877, MT6885, MT6893, MT8167, MT8167S, MT8175, MT8185, MT8195, MT8321, MT8362A, MT8365, MT8385, MT8395, MT8666, MT8667, MT8673, MT8675, MT8678, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8797, MT8798, MT8893
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2024-20142**
Title	Out-of-bounds write in DA
Severity	High
Vulnerability Type	EoP
CWE	CWE-787 Out-of-bounds Write

	execution privileges needed. User interaction is needed for exploitation.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6771, MT6779, MT6781, MT6785, MT6833, MT6853, MT6873, MT6877, MT6885, MT6893, MT8167, MT8167S, MT8175, MT8185, MT8195, MT8321, MT8362A, MT8365, MT8385, MT8395, MT8666, MT8667, MT8673, MT8675, MT8678, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8797, MT8798, MT8893
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2025-20638**
Title	Use of uninitialized variable in Flash Tool V5 DA
Severity	Medium
Vulnerability Type	ID
CWE	CWE-457 Use of Uninitialized Variable

	device, with no additional execution privileges needed. User interaction is needed for exploitation.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6771, MT6779, MT6781, MT6785, MT6833, MT6853, MT6873, MT6877, MT6885, MT6893, MT8167, MT8167S, MT8175, MT8185, MT8195, MT8321, MT8362A, MT8365, MT8385, MT8395, MT8666, MT8667, MT8673, MT8675, MT8678, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8797, MT8798, MT8893
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2025-20639**
Title	Out-of-bounds write in Flash Tool V5 Lib adaptor
Severity	Medium
Vulnerability Type	EoP
CWE	CWE-787 Out-of-bounds Write

	execution privileges needed. User interaction is needed for exploitation.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6771, MT6779, MT6781, MT6785, MT6833, MT6853, MT6873, MT6877, MT6885, MT6893, MT8167, MT8167S, MT8175, MT8185, MT8195, MT8321, MT8362A, MT8365, MT8385, MT8395, MT8666, MT8667, MT8673, MT8675, MT8678, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8797, MT8798, MT8893
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2025-20640**
Title	Out-of-bounds read in Flash Tool V5 Lib adaptor
Severity	Medium
Vulnerability Type	ID
CWE	CWE-125 Out-of-bounds Read

	execution privileges needed. User interaction is needed for exploitation.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6771, MT6779, MT6781, MT6785, MT6833, MT6853, MT6873, MT6877, MT6885, MT6893, MT8167, MT8167S, MT8175, MT8185, MT8195, MT8321, MT8362A, MT8365, MT8385, MT8395, MT8666, MT8667, MT8673, MT8675, MT8678, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8797, MT8798, MT8893
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2025-20641**
Title	Out-of-bounds write in Flash Tool V5 old-arch Lib
Severity	Medium
Vulnerability Type	EoP
CWE	CWE-787 Out-of-bounds Write

	execution privileges needed. User interaction is needed for exploitation.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6771, MT6779, MT6781, MT6785, MT6833, MT6853, MT6873, MT6877, MT6885, MT6893, MT8167, MT8167S, MT8175, MT8185, MT8195, MT8321, MT8362A, MT8365, MT8385, MT8395, MT8666, MT8667, MT8673, MT8675, MT8678, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8797, MT8798, MT8893
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2025-20642**
Title	Out-of-bounds write in Flash Tool V5 old-arch Lib
Severity	Medium
Vulnerability Type	EoP
CWE	CWE-787 Out-of-bounds Write

	execution privileges needed. User interaction is needed for exploitation.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6771, MT6779, MT6781, MT6785, MT6833, MT6853, MT6873, MT6877, MT6885, MT6893, MT8167, MT8167S, MT8175, MT8185, MT8195, MT8321, MT8362A, MT8365, MT8385, MT8395, MT8666, MT8667, MT8673, MT8675, MT8678, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8797, MT8798, MT8893
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2025-20643**
Title	Debug messages revealing unnecessary information in Flash Tool V5 old-arch Lib
Severity	Medium
Vulnerability Type	ID
CWE	CWE-1295 Debug Messages Revealing Unnecessary Information

	has already obtained the System privilege. User interaction is needed for exploitation.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6771, MT6779, MT6781, MT6785, MT6833, MT6853, MT6873, MT6877, MT6885, MT6893, MT8167, MT8167S, MT8175, MT8185, MT8195, MT8321, MT8362A, MT8365, MT8385, MT8395, MT8666, MT8667, MT8673, MT8675, MT8678, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8795T, MT8797, MT8798, MT8893
Affected Software Versions	Android 12.0, 13.0, 14.0, 15.0
Report Source	Internal

CVE	**CVE-2024-20147**
Title	Reachable assertion in Bluetooth
Severity	Medium
Vulnerability Type	DoS
CWE	CWE-617 Reachable Assertion

	User interaction is not needed for exploitation.
Affected Chipsets	MT2737, MT3603, MT6835, MT6878, MT6886, MT6897, MT6985, MT6989, MT6990, MT7902, MT7920, MT7921, MT7922, MT7925, MT7927, MT8195, MT8370, MT8390, MT8395, MT8518S, MT8532, MT8678
Affected Software Versions	Android 13.0, 14.0, 15.0 / SDK release 2.5, 3.5 and before / openWRT 23.05 / Yocto 3.3, 4.0, 5.0
Report Source	Internal

Vulnerability Type Definition

Abbreviation	Definition
RCE	Remote Code Execution
EoP	Elevation of Privilege
ID	Information Disclosure
DoS	Denial of Service
N/A	Classification not available

Versions

Version	Date	Description

Information above is generated only at the time of creation of this Security Bulletin. The list of affected chipsets could be not complete. For any further information, device OEMs can reach your MediaTek contact person if needed.

If you want to report a security vulnerability in MediaTek chipsets or products, please go to Report Security Vulnerability page on MediaTek website.