Announcement

Report Vulnerability

Disclosure Policy

Security Bulletin

Acknowledgements

The MediaTek Product Security Bulletin contains details of security vulnerabilities affecting certain MediaTek chipsets. Device OEMs have been notified of all the issues and the corresponding security patches for at least two months before publication. We take the security of our chipsets and our customers' products very seriously. At this time, we are not aware of any active exploitation of these vulnerabilities in the wild.

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

Summary

Severity	CVEs
High	CVE-2025-20795, CVE-2025-20794, CVE-2025-20793, CVE-2025-20762, CVE-2025-20761, CVE-2025-20760

	CVE-2025-20802, CVE-2025-20778, CVE-2025-20779, CVE-2025-20780, CVE-2025-20781, CVE-2025-20782, CVE-2025-20783, CVE-2025-20784, CVE-2025-20785, CVE-2025-20786, CVE-2025-20787, CVE-2025-20803, CVE-2025-20804, CVE-2025-20805, CVE-2025-20806, CVE-2025-20807

Details

CVE	**CVE-2025-20795**
Title	Out-of-bounds write in KeyInstall
Severity	High
CWE	CWE-787 Out-of-bounds Write
Description	There is a possible out of bounds write due to a missing bounds check.
Affected Chipsets	MT2718, MT6580, MT6739, MT6761, MT6765, MT6768, MT6779, MT6781, MT6785, MT6789, MT6833, MT6835, MT6853, MT6855, MT6873, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8195, MT8196, MT8370, MT8390, MT8391, MT8395, MT8676, MT8678, MT8696, MT8755, MT8766, MT8768, MT8781, MT8786, MT8788E, MT8791T, MT8792, MT8793, MT8796, MT8873, MT8883, MT8893
Report Source	External

CVE	**CVE-2025-20794**
Title	Stack overflow in Modem

CWE	CWE-121 Stack Overflow
Description	There is a possible system crash due to improper input validation.
Affected Chipsets	MT2735, MT2737, MT6813, MT6815, MT6833, MT6835, MT6853, MT6855, MT6873, MT6875, MT6877, MT6878, MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6896, MT6897, MT6899, MT6980, MT6983, MT6985, MT6986, MT6989, MT6990, MT6991, MT6993, MT8673, MT8675, MT8676, MT8678, MT8755, MT8771, MT8791, MT8791T, MT8792, MT8793, MT8795T, MT8797, MT8798, MT8863, MT8873, MT8883, MT8893
Report Source	External

CVE	**CVE-2025-20793**
Title	Null pointer dereference in Modem
Severity	High
CWE	CWE-476 NULL Pointer Dereference
Description	There is a possible system crash due to incorrect error handling.

	MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6896, MT6897, MT6899, MT6980, MT6983, MT6985, MT6989, MT6990, MT6991, MT6993, MT8673, MT8675, MT8676, MT8678, MT8755, MT8771, MT8791, MT8791T, MT8792, MT8793, MT8795T, MT8797, MT8798, MT8863, MT8873, MT8883, MT8893
Report Source	External

CVE	**CVE-2025-20762**
Title	Reachable assertion in Modem
Severity	High
CWE	CWE-617 Reachable Assertion
Description	There is a possible system crash due to incorrect error handling.
Affected Chipsets	MT6835, MT6835T, MT6878, MT6878M, MT6897, MT6899, MT6991, MT8676, MT8678, MT8755, MT8792, MT8793, MT8863, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20761**
Title	Improper check for unusual or exceptional conditions in Modem
Severity	High

Description	There is a possible system crash due to incorrect error handling.
Affected Chipsets	MT2735, MT2737, MT6833, MT6833P, MT6835, MT6835T, MT6853, MT6853T, MT6855, MT6855T, MT6873, MT6875, MT6875T, MT6877, MT6877T, MT6877TT, MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6895TT, MT6896, MT6897, MT6980, MT6980D, MT6983, MT6983T, MT6985, MT6985T, MT6989, MT6989T, MT6990, MT8673, MT8675, MT8676, MT8678, MT8755, MT8771, MT8791, MT8791T, MT8792, MT8793, MT8795T, MT8797, MT8798, MT8863, MT8873, MT8883, MT8893
Report Source	External

CVE	**CVE-2025-20760**
Title	Reachable assertion in Modem
Severity	High
CWE	CWE-617 Reachable Assertion
Description	There is a possible read of uninitialized heap data due to an uncaught exception.
Affected Chipsets	MT2735, MT2737, MT6833, MT6835, MT6853, MT6855, MT6873, MT6875, MT6877, MT6878, MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6896, MT6897, MT6899, MT6980, MT6983, MT6985, MT6986, MT6989, MT6990, MT6991, MT6993, MT8673, MT8675, MT8676, MT8678, MT8755, MT8771, MT8791, MT8791T, MT8792, MT8793, MT8795T, MT8797, MT8798, MT8863, MT8873, MT8883, MT8893

CVE	CVE-2025-20796
Title	Specified index, position, or offset in imgsys
Severity	Medium
CWE	CWE-1285 Specified Index, Position, or Offset
Description	There is a possible out of bounds write due to improper input validation.
Affected Chipsets	MT6989, MT8796, MT8893
Report Source	External

CVE	CVE-2025-20797
Title	Stack overflow in battery
Severity	Medium
CWE	CWE-121 Stack Overflow
Description	There is a possible out of bounds write due to a missing bounds check.
Affected Chipsets	MT2718, MT6765, MT6768, MT6781, MT6833, MT6835, MT6853, MT6855, MT6877, MT6879, MT6893, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8367, MT8391, MT8676, MT8678, MT8696, MT8766, MT8768, MT8781, MT8786, MT8788E, MT8791T, MT8792, MT8793, MT8796, MT8873, MT8883, MT8893
Report Source	External

Title	Out-of-bounds write in battery
Severity	Medium
CWE	CWE-787 Out-of-bounds Write
Description	There is a possible out of bounds write due to a missing bounds check.
Affected Chipsets	MT2718, MT6765, MT6768, MT6781, MT6833, MT6835, MT6853, MT6855, MT6877, MT6879, MT6893, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8367, MT8391, MT8676, MT8678, MT8696, MT8766, MT8768, MT8781, MT8786, MT8788E, MT8791T, MT8792, MT8793, MT8796, MT8873, MT8883, MT8893
Report Source	External

CVE	**CVE-2025-20799**
Title	Use after free in c2ps
Severity	Medium
CWE	CWE-416 Use After Free
Description	There is a possible memory corruption due to use after free.
Affected Chipsets	MT6899, MT6991, MT6993, MT8793
Report Source	External

CVE	**CVE-2025-20800**

Severity	Medium
CWE	CWE-787 Out-of-bounds Write
Description	There is a possible out of bounds write due to a missing bounds check.
Affected Chipsets	MT2718, MT6899, MT6989, MT6991, MT8678, MT8793
Report Source	External

CVE	**CVE-2025-20801**
Title	Double free in seninf
Severity	Medium
CWE	CWE-415 Double Free
Description	There is a possible memory corruption due to a race condition.
Affected Chipsets	MT6878, MT6897, MT6899, MT6985, MT6989, MT6991, MT6993, MT8792, MT8796, MT8798
Report Source	External

CVE	**CVE-2025-20802**
Title	Use after free in geniezone
Severity	Medium
CWE	CWE-416 Use After Free

Affected Chipsets	MT6991, MT8196, MT8367, MT8781, MT8786, MT8793
Report Source	External

CVE	**CVE-2025-20778**
Title	Out-of-bounds write in display
Severity	Medium
CWE	CWE-787 Out-of-bounds Write
Description	There is a possible out of bounds write due to a missing bounds check.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20779**
Title	Use after free in display
Severity	Medium
CWE	CWE-416 Use After Free

Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20780**
Title	Use after free in display
Severity	Medium
CWE	CWE-416 Use After Free
Description	There is a possible memory corruption due to use after free.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20781**
Title	Double free in display

CWE	CWE-415 Double Free
Description	There is a possible memory corruption due to use after free.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20782**
Title	Out-of-bounds write in display
Severity	Medium
CWE	CWE-787 Out-of-bounds Write
Description	There is a possible out of bounds write due to a missing bounds check.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883

CVE	**CVE-2025-20783**
Title	Out-of-bounds write in display
Severity	Medium
CWE	CWE-787 Out-of-bounds Write
Description	There is a possible out of bounds write due to a missing bounds check.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20784**
Title	Use of uninitialized variable in display
Severity	Medium
CWE	CWE-457 Use of Uninitialized Variable
Description	There is a possible memory corruption due to uninitialized data.

	MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20785**
Title	Use after free in display
Severity	Medium
CWE	CWE-416 Use After Free
Description	There is a possible memory corruption due to use after free.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20786**
Title	Double free in display
Severity	Medium

Description	There is a possible memory corruption due to use after free.
Affected Chipsets	MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8186, MT8188, MT8196, MT8667, MT8673, MT8676, MT8678, MT8765, MT8766, MT8768, MT8771, MT8781, MT8791T, MT8792, MT8793, MT8795T, MT8796, MT8798, MT8873, MT8883
Report Source	External

CVE	**CVE-2025-20787**
Title	Use after free in display
Severity	Medium
CWE	CWE-416 Use After Free
Description	There is a possible memory corruption due to use after free.
Affected Chipsets	MT2718, MT6739, MT6761, MT6765, MT6768, MT6781, MT6789, MT6833, MT6835, MT6853, MT6855, MT6877, MT6878, MT6879, MT6883, MT6885, MT6886, MT6889, MT6893, MT6895, MT6897, MT6899, MT6983, MT6985, MT6989, MT6991, MT8196, MT8676, MT8678, MT8796
Report Source	External

CVE	**CVE-2025-20803**

Severity	Medium
CWE	CWE-190 Integer Overflow
Description	There is a possible memory corruption due to an integer overflow.
Affected Chipsets	MT6899, MT6991, MT8793
Report Source	External

CVE	**CVE-2025-20804**
Title	Use after free in dpe
Severity	Medium
CWE	CWE-416 Use After Free
Description	There is a possible memory corruption due to use after free.
Affected Chipsets	MT6899, MT6991
Report Source	External

CVE	**CVE-2025-20805**
Title	Use after free in dpe
Severity	Medium
CWE	CWE-416 Use After Free

Affected Chipsets	MT6899, MT6991, MT8793
Report Source	External

CVE	**CVE-2025-20806**
Title	Use after free in dpe
Severity	Medium
CWE	CWE-416 Use After Free
Description	There is a possible memory corruption due to use after free.
Affected Chipsets	MT6899, MT6991, MT8793
Report Source	External

CVE	**CVE-2025-20807**
Title	Integer overflow in dpe
Severity	Medium
CWE	CWE-190 Integer Overflow
Description	There is a possible out of bounds write due to an integer overflow.
Affected Chipsets	MT6899, MT6991, MT8793
Report Source	External

1.0	January 5, 2026	Bulletin published.

Notes

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.