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-2026-20447, CVE-2026-20448, CVE-2026-20449, CVE-2026-20450

Details

CVE	**CVE-2026-20447**
Subcomponent	geniezone
Severity	High
CWE	CWE-125 Out-of-bounds Read
Description	There is a possible escalation of privilege due to a missing bounds check.
Affected Chipsets	MT6768, MT6789, MT6877, MT6899, MT6989, MT6991, MT6993, MT8196, MT8367, MT8766, MT8768, MT8781, MT8786, MT8788E, MT8791T, MT8793, MT8910
Report Source	External

CVE	**CVE-2026-20448**
Subcomponent	geniezone
Severity	High
CWE	CWE-280 Improper Handling of Insufficient Permissions or Privileges
Description	There is a possible escalation of privilege due to a missing permission check.
Affected Chipsets	MT6765, MT6768, MT6789, MT6877, MT6897, MT6899, MT6989, MT6991, MT6993, MT8367, MT8766, MT8768, MT8775, MT8781, MT8786, MT8788E, MT8791T, MT8792, MT8793, MT8796, MT8893, MT8910

CVE	CVE-2026-20449
Subcomponent	Modem
Severity	High
CWE	CWE-120 Classic Buffer Overflow
Description	There is a possible system crash due to a heap buffer overflow.
Affected Chipsets	MT2735, MT2737, MT6739, MT6761, MT6762, MT6763, MT6765, MT6767, MT6768, MT6769, MT6771, MT6779, MT6781, MT6783, MT6785, MT6789, MT6813, MT6815, MT6833, MT6835, MT6853, MT6855, MT6858, MT6873, MT6875, MT6877, MT6878, MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6896, MT6897, MT6899, MT6980, MT6983, MT6985, MT6986D, MT6988, MT6989, MT6990, MT6991, MT6993, MT8668, MT8673, MT8675, MT8676, MT8678, MT8755, MT8771, MT8775, MT8791, MT8791T, MT8792, MT8793, MT8795T, MT8797, MT8798, MT8863, MT8873, MT8883, MT8893
Report Source	External

CVE	CVE-2026-20450
Subcomponent	Modem
Severity	High
CWE	CWE-617 Reachable Assertion

Affected Chipsets	MT2735, MT2737, MT6833, MT6835, MT6853, MT6855, MT6858, 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, MT8668, MT8673, MT8675, MT8676, MT8678, MT8755, MT8771, MT8775, MT8791, MT8791T, MT8792, MT8793, MT8795T, MT8797, MT8798, MT8863, MT8873, MT8883, MT8893
Report Source	Internal

CVE	**CVE-2026-20451**
Subcomponent	slbc
Severity	Medium
CWE	CWE-843 Access of Resource Using Incompatible Type ('Type Confusion')
Description	There is a possible out of bounds write due to type confusion.
Affected Chipsets	MT2718, MT6899, MT6985, MT6989, MT6991, MT8115, MT8186, MT8188, MT8196, MT8365, MT8367, MT8370, MT8371, MT8390, MT8391, MT8395, MT8676, MT8678, MT8766, MT8768, MT8775, MT8781, MT8786, MT8788E, MT8791T, MT8792, MT8793, MT8796, MT8873, MT8883, MT8893, MT8910
Report Source	External

Versions

1.0	May 4, 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.