

[Announcement](#)[Report Vulnerability](#)[Disclosure Policy](#)[Security Bulletin](#)[Acknowledgements](#)

# April 2026 Product Security Bulletin

Published 2026-04-07

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-2026-20431, CVE-2026-20432, CVE-2026-20433

**Details**

<b>CVE</b>	<b>CVE-2026-20431</b>
<b>Subcomponent</b>	Modem
<b>Severity</b>	High
<b>CWE</b>	CWE-770 Allocation of Resources Without Limits or Throttling
<b>Description</b>	There is a possible system crash due to a logic error.
<b>Affected Chipsets</b>	MT6813, MT6815, MT6835, MT6878, MT6897, MT6899, MT6986, MT6991, MT6993, MT8668, MT8676, MT8678, MT8755, MT8775, MT8792, MT8793, MT8863, MT8873, MT8883
<b>Report Source</b>	Internal

<b>CVE</b>	<b>CVE-2026-20432</b>
<b>Subcomponent</b>	Modem
<b>Severity</b>	High
<b>CWE</b>	CWE-787 Out-of-bounds Write
<b>Description</b>	There is a possible out of bounds write due to a missing bounds check.



	MT6855, MT6873, MT6875, MT6877, MT6878, MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6896, MT6897, MT6899, MT6980, MT6983, MT6985, MT6989, MT6990, MT6991, MT6993, MT8668, MT8673, MT8675, MT8676, MT8678, MT8755, MT8771, MT8775, MT8781, MT8789, MT8791, MT8791T, MT8792, MT8793, MT8795T, MT8797, MT8798, MT8863, MT8873, MT8883, MT8893
<b>Report Source</b>	Internal

<b>CVE</b>	<b>CVE-2026-20433</b>
<b>Subcomponent</b>	Modem
<b>Severity</b>	High
<b>CWE</b>	CWE-787 Out-of-bounds Write
<b>Description</b>	There is a possible out of bounds write due to a missing bounds check.
<b>Affected Chipsets</b>	MT2735, MT2737, MT6813, MT6833, MT6833P, MT6835, MT6835T, MT6853, MT6853T, MT6855, MT6855T, MT6873, MT6875, MT6875T, MT6877, MT6877T, MT6877TT, MT6878, MT6878M, MT6879, MT6880, MT6883, MT6885, MT6886, MT6889, MT6890, MT6891, MT6893, MT6895, MT6895TT, MT6896, MT6897, MT6899, MT6980, MT6980D, MT6983, MT6983T, MT6985, MT6985T, MT6989, MT6989T, MT6990, MT6991, MT8668, MT8673, MT8675, MT8676, MT8678, MT8755, MT8771, MT8775, MT8791, MT8791T, MT8792, MT8793, MT8795T, MT8797, MT8798, MT8863, MT8873, MT8883, MT8893
<b>Report Source</b>	Internal



<b>Subcomponent</b>	sec boot
<b>Severity</b>	Medium
<b>CWE</b>	CWE-787 Out-of-bounds Write
<b>Description</b>	There is a possible out of bounds write due to an integer overflow.
<b>Affected Chipsets</b>	MT6813
<b>Report Source</b>	Internal

### Versions

Version	Date	Description
1.0	April 7, 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.

**ABOUT MEDIATEK**



**NEWS**





## JOIN OUR NEWSLETTER

SUBMIT



[Cookie Statement](#)

[Legal Notice](#)

[Privacy Policy](#)

© 2026 MediaTek Inc. All Rights Reserved