



CVE-2022-32656

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2022-32656 |
| State | PUBLIC |
| Assigner | security@mediatek.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-02-06 20:15:00 UTC |
| Updated | 2023-02-14 18:53:00 UTC |
| Description | In Wi-Fi driver, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of p |

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------|---------------------------------|---------|--------|---------|----------|
| Hardware | Mediatek | Mt5221 | - | All | All | All |
| Operating System | Mediatek | Mt5221 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7603 | - | All | All | All |
| Operating System | Mediatek | Mt7603 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7613 | - | All | All | All |
| Operating System | Mediatek | Mt7613 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7615 | - | All | All | All |
| Operating System | Mediatek | Mt7615 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7622 | - | All | All | All |
| Operating System | Mediatek | Mt7622 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7628 | - | All | All | All |
| Operating System | Mediatek | Mt7628 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7629 | - | All | All | All |
| Operating System | Mediatek | Mt7629 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7663 | - | All | All | All |
| Operating System | Mediatek | Mt7663 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7668 | - | All | All | All |

| | | | | | | |
|------------------|--------------------------|----------------------------------|---------|-----|-----|-----|
| Operating System | Mediatek | Mt7668 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7682 | - | All | All | All |
| Operating System | Mediatek | Mt7682 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7686 | - | All | All | All |
| Operating System | Mediatek | Mt7686 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7687 | - | All | All | All |
| Operating System | Mediatek | Mt7687 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7697 | - | All | All | All |
| Operating System | Mediatek | Mt7697 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7902 | - | All | All | All |
| Operating System | Mediatek | Mt7902 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7915 | - | All | All | All |
| Operating System | Mediatek | Mt7915 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7916 | - | All | All | All |
| Operating System | Mediatek | Mt7916 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7921 | - | All | All | All |
| Operating System | Mediatek | Mt7921 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7933 | - | All | All | All |
| Operating System | Mediatek | Mt7933 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7981 | - | All | All | All |
| Operating System | Mediatek | Mt7981 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt7986 | - | All | All | All |
| Operating System | Mediatek | Mt7986 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8167s | - | All | All | All |
| Operating System | Mediatek | Mt8167s Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8175 | - | All | All | All |
| Operating System | Mediatek | Mt8175 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8362a | - | All | All | All |
| Operating System | Mediatek | Mt8362a Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8365 | - | All | All | All |
| Operating System | Mediatek | Mt8365 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8385 | - | All | All | All |
| Operating System | Mediatek | Mt8385 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8518s | - | All | All | All |
| Operating System | Mediatek | Mt8518s Firmware | 7.6.6.0 | All | All | All |

| | | | | | | |
|------------------|--------------------------|---------------------------------|---------|-----|-----|-----|
| Hardware | Mediatek | Mt8532 | - | All | All | All |
| Operating System | Mediatek | Mt8532 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8695 | - | All | All | All |
| Operating System | Mediatek | Mt8695 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8696 | - | All | All | All |
| Operating System | Mediatek | Mt8696 Firmware | 7.6.6.0 | All | All | All |
| Hardware | Mediatek | Mt8788 | - | All | All | All |
| Operating System | Mediatek | Mt8788 Firmware | 7.6.6.0 | All | All | All |

References

| Reference | Source | Link | Tags |
|--------------------------|---------|--|---------------------|
| February 2023 | MISC | corp.mediatek.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report