



CVE-2022-20025

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

Summary

CVE	CVE-2022-20025
State	PUBLIC
Assigner	security@mediatek.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-09 23:15:00 UTC
Updated	2022-02-11 20:26:00 UTC
Description	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of pr

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	10.0	All	All	All
Operating System	Google	Android	11.0	All	All	All
Operating System	Google	Android	12.0	All	All	All
Operating System	Google	Android	8.1	All	All	All
Operating System	Google	Android	9.0	All	All	All
Hardware	Mediatek	Mt8167	-	All	All	All
Hardware	Mediatek	Mt8175	-	All	All	All
Hardware	Mediatek	Mt8183	-	All	All	All
Hardware	Mediatek	Mt8362a	-	All	All	All
Hardware	Mediatek	Mt8365	-	All	All	All
Hardware	Mediatek	Mt8385	-	All	All	All

References

Reference	Source	Link	Tags
February 2022	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.

Legacy QID Mappings

610397 Google Android Devices February 2022 Security Patch Missing

© [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](#)