



CVE-2022-20044

Published on: 02/09/2022 12:00:00 AM UTC

Last Modified on: 02/14/2022 08:20:00 PM UTC

CVE-2022-20044

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814.

CVE-2022-20044 has been assigned by [security@mediatek.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [MediaTek, Inc.](#) - MT8167, MT8175, MT8183, MT8362A, MT8365, MT8385 version **Android 8.1, 9.0, 10.0, 11.0, 12.0**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
February 2022	corp.mediatek.com text/html	MISC corp.mediatek.com/product-security-bulletin/February-2022

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:o:google:android:10.0:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:o:google:android:11.0:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:o:google:android:12.0:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:o:google:android:8.1:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:o:google:android:9.0:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:mediatek:mt8167:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:mediatek:mt8175:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:mediatek:mt8183:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:mediatek:mt8362a:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:mediatek:mt8365:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:h:mediatek:mt8385:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-20044 : In Bluetooth, there is a possible service crash due to a use after free. This could lead to local... twitter.com/i/web/status/1...	2022-02-09 23:14:49

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)