



CVE-2023-20691

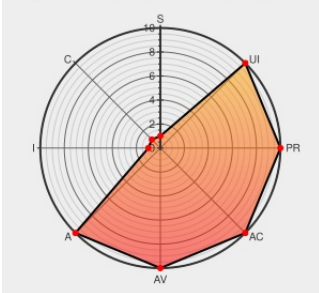
Published on: Not Yet Published

Last Modified on: 07/07/2023 11:52:00 PM UTC

CVE-2023-20691

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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

In wlan firmware, there is possible system crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664731; Issue ID: ALPS07664731.

CVE-2023-20691 has been assigned by [security@mediatek.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [MediaTek, Inc.](#) - **MT6739, MT8167, MT8321, MT8365, MT8385, MT8666, MT8765, MT8788** version = **Android 11.0, 12.0 / IOT-v23.0 (Yocto 4.0)**

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
July 2023	corp.mediatek.com text/html	MISC corp.mediatek.com/product-security-bulletin/July-2023

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	11.0	All	All	All
Operating System	Google	Android	12.0	All	All	All
Application	Linuxfoundation	Yocto	4.0	All	All	All
Hardware  	Mediatek	Mt6739	-	All	All	All
Hardware  	Mediatek	Mt8167	-	All	All	All
Hardware  	Mediatek	Mt8321	-	All	All	All
Hardware  	Mediatek	Mt8365	-	All	All	All
Hardware  	Mediatek	Mt8385	-	All	All	All
Hardware  	Mediatek	Mt8666	-	All	All	All
Hardware  	Mediatek	Mt8765	-	All	All	All
Hardware  	Mediatek	Mt8788	-	All	All	All
cpe:2.3:o:google:android:11.0:*****:						
cpe:2.3:o:google:android:12.0:*****:						
cpe:2.3:a:linuxfoundation:yocto:4.0:*****:						
cpe:2.3:h:mediatek:mt6739:-:*****:						
cpe:2.3:h:mediatek:mt8167:-:*****:						
cpe:2.3:h:mediatek:mt8321:-:*****:						
cpe:2.3:h:mediatek:mt8365:-:*****:						
cpe:2.3:h:mediatek:mt8385:-:*****:						
cpe:2.3:h:mediatek:mt8666:-:*****:						
cpe:2.3:h:mediatek:mt8765:-:*****:						
cpe:2.3:h:mediatek:mt8788:-:*****:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
 @CVEreport	CVE-2023-20691 : In wlan firmware, there is possible system crash due to an integer overflow. This could lead to re... twitter.com/i/web/status/1...					2023-07-04 02:08:12

© [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](#)