

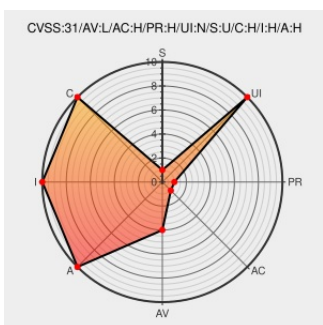


CVE-2023-20611

Published on: Not Yet Published

Last Modified on: 02/14/2023 05:39:00 PM UTC

CVE-2023-20611

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

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

In gpu, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588678; Issue ID: ALPS07588678.

CVE-2023-20611 has been assigned by [security@mediatek.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [MediaTek, Inc.](#) - MT6580, MT6731, MT6735, MT6737, MT6739, MT6753, MT6757, MT6757C, MT6757CD, MT6757CH, MT6761, MT6762, MT6763, MT6765, MT6768, MT6769, MT6771, MT6779, MT6781, MT6785, MT6789, MT6833, MT6853, MT6853T, MT6855, MT6873, MT6875, MT6877, MT6879, MT6883, MT6885, MT6889, MT6891, MT6893, MT6895, MT6983, MT8168, MT8365 version **Android 12.0, 13.0**

CVSS3 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
February 2023	corp.mediatek.com text/html	MISC corp.mediatek.com/product-security-bulletin/February-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 OIDs associated with this CVE

There are currently no CVEs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	12.0	All	All	All
Operating System	Google	Android	13.0	All	All	All
Hardware  	Mediatek	Mt6580	-	All	All	All
Hardware  	Mediatek	Mt6731	-	All	All	All
Hardware  	Mediatek	Mt6735	-	All	All	All
Hardware  	Mediatek	Mt6737	-	All	All	All
Hardware  	Mediatek	Mt6739	-	All	All	All
Hardware  	Mediatek	Mt6753	-	All	All	All
Hardware  	Mediatek	Mt6757	-	All	All	All
Hardware  	Mediatek	Mt6757c	-	All	All	All
Hardware  	Mediatek	Mt6757cd	-	All	All	All
Hardware  	Mediatek	Mt6757ch	-	All	All	All
Hardware  	Mediatek	Mt6761	-	All	All	All
Hardware  	Mediatek	Mt6762	-	All	All	All
Hardware  	Mediatek	Mt6763	-	All	All	All
Hardware  	Mediatek	Mt6765	-	All	All	All
Hardware  	Mediatek	Mt6768	-	All	All	All
Hardware  	Mediatek	Mt6769	-	All	All	All
Hardware  	Mediatek	Mt6771	-	All	All	All
Hardware  	Mediatek	Mt6779	-	All	All	All
Hardware  	Mediatek	Mt6781	-	All	All	All
Hardware  	Mediatek	Mt6785	-	All	All	All
Hardware  	Mediatek	Mt6789	-	All	All	All
Hardware  	Mediatek	Mt6833	-	All	All	All
Hardware  	Mediatek	Mt6853	-	All	All	All
Hardware  	Mediatek	Mt6853t	-	All	All	All
Hardware  	Mediatek	Mt6855	-	All	All	All
Hardware  	Mediatek	Mt6873	-	All	All	All

Hardware		Mediatek	Mt6875	-	All	All	All
Hardware		Mediatek	Mt6877	-	All	All	All
Hardware		Mediatek	Mt6879	-	All	All	All
Hardware		Mediatek	Mt6883	-	All	All	All
Hardware		Mediatek	Mt6885	-	All	All	All
Hardware		Mediatek	Mt6889	-	All	All	All
Hardware		Mediatek	Mt6891	-	All	All	All
Hardware		Mediatek	Mt6893	-	All	All	All
Hardware		Mediatek	Mt6895	-	All	All	All
Hardware		Mediatek	Mt6983	-	All	All	All
Hardware		Mediatek	Mt8168	-	All	All	All
Hardware		Mediatek	Mt8365	-	All	All	All
cpe:2.3:o:google:android:12.0:*****:							
cpe:2.3:o:google:android:13.0:*****:							
cpe:2.3:h:mediatek:mt6580:-:*****:							
cpe:2.3:h:mediatek:mt6731:-:*****:							
cpe:2.3:h:mediatek:mt6735:-:*****:							
cpe:2.3:h:mediatek:mt6737:-:*****:							
cpe:2.3:h:mediatek:mt6739:-:*****:							
cpe:2.3:h:mediatek:mt6753:-:*****:							
cpe:2.3:h:mediatek:mt6757:-:*****:							
cpe:2.3:h:mediatek:mt6757c:-:*****:							
cpe:2.3:h:mediatek:mt6757cd:-:*****:							
cpe:2.3:h:mediatek:mt6757ch:-:*****:							
cpe:2.3:h:mediatek:mt6761:-:*****:							
cpe:2.3:h:mediatek:mt6762:-:*****:							
cpe:2.3:h:mediatek:mt6763:-:*****:							
cpe:2.3:h:mediatek:mt6765:-:*****:							
cpe:2.3:h:mediatek:mt6768:-:*****:							

cpe:2.3:h:mediatek:mt6769:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6771:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6779:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6781:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6785:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6789:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6833:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6853:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6853t:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6855:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6873:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6875:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6877:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6879:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6883:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6885:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6889:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6891:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6893:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6895:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt6983:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt8168:-:~::~~::~~::~~::~~::~~::~~::
cpe:2.3:h:mediatek:mt8365:-:~::~~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVereport	CVE-2023-20611 : In gpu, there is a possible use after free due to a race condition. This could lead to local escal... twitter.com/i/web/status/1...	2023-02-06 20:18:16
	MediaTek Android privilege escalation CVE-2023-20611 - redpacketsecurity.com/mediatek-andro...	2023-02-12

[← 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](#)