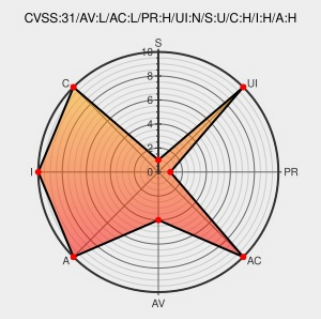
CVE-2022-32646

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-32646

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Android from Google contain the following vulnerability:

In gpu drm, there is a possible stack overflow due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07363501; Issue ID: ALPS07363501.

CVE-2022-32646 has been assigned by security@mediatek.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **MediaTek, Inc.** - **MT6761, MT6765, MT6768, MT6779, MT6781, MT6785, MT6789, MT6833, MT6853, MT6855, MT6873, MT6877, MT6879, MT6883, MT6885, MT6889, MT6893, MT6895, MT6983, MT8675, MT8766, MT8781, MT8791** version **Android 11.0, 12.0, 13.0**

CVSS3 Score: 6.7 - MEDIUM

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

CVE References

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

Exploit/POC from Github

In gpu drm, there is a possible stack overflow due to a missing bounds check. This could lead to local escalation of …

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
Operating System	Google	Android	13.0	All	All	All
Hardware	Mediatek	Mt6761	-	All	All	All
Hardware	Mediatek	Mt6765	-	All	All	All
Hardware	Mediatek	Mt6768	-	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	Mt6855	-	All	All	All
Hardware	Mediatek	Mt6873	-	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	Mt6893	-	All	All	All
Hardware	Mediatek	Mt6895	-	All	All	All
Hardware	Mediatek	Mt6983	-	All	All	All
Hardware	Mediatek	Mt8675	-	All	All	All
Hardware	Mediatek	Mt8766	-	All	All	All

Hardware	Mediatek	Mt8781	-	All	All	All
Hardware	Mediatek	Mt8791	-	All	All	All

cpe:2.3:o:google:android:11.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:12.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:13.0:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt6761:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt6765:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt6768:-:*:*:*:*:*:*:*:

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:mt6855:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt6873:-:*:*:*:*:*:*:*:

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:mt6893:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt6895:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt6983:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt8675:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt8766:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt8781:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt8791:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-32646 : In gpu drm, there is a possible stack overflow due to a missing bounds check. This could lead to l… twitter.com/i/web/status/1…	2023-01-03 21:08:00
/r/netcve	CVE-2022-32646	2023-01-03 21:38:47

← Previous ID

Next ID→