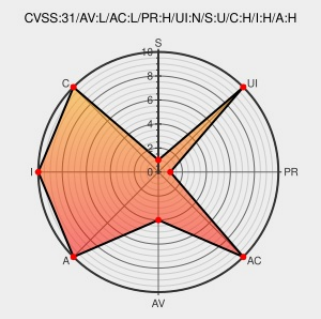
CVE-2023-20614

Published on: Not Yet Published

Last Modified on: 02/14/2023 05:50:00 PM UTC

CVE-2023-20614

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



Certain versions of Android from Google contain the following vulnerability:

In ril, there is a possible out of bounds write 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: ALPS07628615; Issue ID: ALPS07628615.

CVE-2023-20614 has been assigned by security@mediatek.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **MediaTek, Inc.** - **MT6739, MT6761, MT6762, MT6765, MT6768, MT6769, MT6771, MT6779, MT6781, MT6785, MT6789, MT6833, MT6853, MT6853T, MT6855, MT6873, MT6875, MT6877, MT6879, MT6883, MT6885, MT6889, MT6891, MT6893, MT6895, MT6983, MT8321, MT8385, MT8765, MT8766, MT8768, MT8786, MT8788, MT8789, MT8791, MT8791T, MT8797** 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
February 2023	corp.mediatek.com text/html	MISC corp.mediatek.com/product-security-bulletin/February-2023

There are currently no OIDs associated with this CVE

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
Operating System	Google	Android	13.0	All	All	All
Hardware	Mediatek	Mt6739	-	All	All	All
Hardware	Mediatek	Mt6761	-	All	All	All
Hardware	Mediatek	Mt6762	-	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	Mt8321	-	All	All	All
Hardware	Mediatek	Mt8385	-	All	All	All
Hardware	Mediatek	Mt8765	-	All	All	All
Hardware	Mediatek	Mt8766	-	All	All	All
Hardware	Mediatek	Mt8768	-	All	All	All
Hardware	Mediatek	Mt8786	-	All	All	All
Hardware	Mediatek	Mt8788	-	All	All	All
Hardware	Mediatek	Mt8789	-	All	All	All
Hardware	Mediatek	Mt8791	-	All	All	All
Hardware	Mediatek	Mt8791t	-	All	All	All
Hardware	Mediatek	Mt8797	-	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:mt6739:-:*:*:*:*:*:*:*:

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

cpe:2.3:h:mediatek:mt6762:-:*:*:*:*:*:*:*:

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:mt8321:-:*:*:*:*:*:*:*:

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

cpe:2.3:h:mediatek:mt8765:-:*:*:*:*:*:*:*:

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

cpe:2.3:h:mediatek:mt8768:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt8786:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt8788:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt8789:-:*:*:*:*:*:*:*:

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

cpe:2.3:h:mediatek:mt8791t:-:*:*:*:*:*:*:*:

cpe:2.3:h:mediatek:mt8797:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-20614 : In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to… twitter.com/i/web/status/1…	2023-02-06 20:19:16

@RedPacketSec	MediaTek Android privilege escalation | CVE-2023-20614 - redpacketsecurity.com/mediatek-andro… #CVE #Vulnerability #OSINT #ThreatIntel #Cyber	2023-02-12 10:03:22

← Previous ID

Next ID→