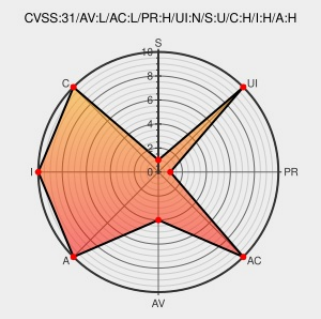
CVE-2021-0655

Published on: 11/18/2021 12:00:00 AM UTC

Last Modified on: 06/28/2022 02:11:00 PM UTC

CVE-2021-0655

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



Certain versions of Android from Google contain the following vulnerability:

In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05673424; Issue ID: ALPS05673424.

CVE-2021-0655 has been assigned by security@android.com to track the vulnerability - currently rated as MEDIUM severity.

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

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
November 2021	corp.mediatek.com text/html	MISC corp.mediatek.com/product-security-bulletin/November-2021

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

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
Hardware	Mediatek	Mt6873	-	All	All	All
Hardware	Mediatek	Mt6875	-	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

cpe:2.3:o:google:android:10.0:*:*:*:*:*:*:*:

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

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

cpe:2.3:h:mediatek:mt6875:-:*:*:*:*:*:*:*:

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:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-0655 : In mdlactl driver, there is a possible memory corruption due to an incorrect bounds check. This cou… twitter.com/i/web/status/1…	2021-11-18 15:10:36

← Previous ID

Next ID→