

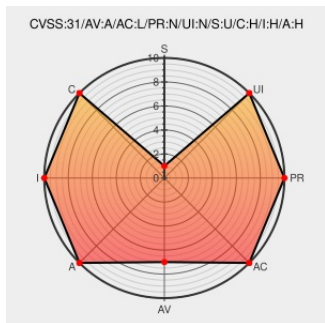


CVE-2023-35684

Published on: Not Yet Published

Last Modified on: 09/14/2023 02:02:00 AM UTC

CVE-2023-35684

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

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

In `avdt_msg_asmb1` of `avdt_msg.cc`, there is a possible out of bounds write due to an integer overflow. This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

CVE-2023-35684 has been assigned by [security@android.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Google](#) - **Android** version = **13**

Affected Vendor/Software: [Google](#) - **Android** version = **12L**

Affected Vendor/Software: [Google](#) - **Android** version = **12**

Affected Vendor/Software: [Google](#) - **Android** version = **11**

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
Android Security Bulletin—September 2023 Android Open Source Project	source.android.com text/html	MISC source.android.com/security/bulletin/2023-09-01
668bbca29797728004d88db4c9b69102f3939008 - platform/packages/modules/Bluetooth - Git at Google	android.googlesource.com text/html	MISC android.googlesource.com/platform/packages/modules/Bluetooth

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
Operating System	Google	Android	12.1	All	All	All
Operating System	Google	Android	13.0	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:12.1:*****:						
cpe:2.3:o:google:android:13.0:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)