



CVE-2023-20965

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-20965
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-14 21:15:00 UTC
Updated	2023-08-24 15:09:00 UTC
Description	In processMessageImpl of ClientModelImpl.java, there is a possible credential disclosure in the TOFU flow due to a logic error

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	13.0	-	All	All

References

Reference	Source	Link
bd318b9772759546509f6fdb8648366099dd65ad - platform/packages/modules/Wifi - Git at Google	MISC	android.googlesource.com
88a8a98934215f591605028e200b6eca8f7cc45a - platform/packages/modules/Wifi - Git at Google	MISC	android.googlesource.com
0d3cb609b0851ea9e5745cc6101e57c2e5e739f2 - platform/packages/modules/Wifi - Git at Google	MISC	android.googlesource.com
Android Security Bulletin—August 2023 Android Open Source Project	MISC	source.android.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[610500](#) Google Android Devices August 2023 Security Patch Missing

[610501](#) Google Android August 2023 Security Patch Missing for Samsung

© [CVE.report](#) 2026 |

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](#)