



# CVE-2023-21297

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

## Summary

<b>CVE</b>	CVE-2023-21297
<b>State</b>	PUBLIC
<b>Assigner</b>	security@android.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-30 17:15:00 UTC
<b>Updated</b>	2023-11-06 17:36:00 UTC
<b>Description</b>	In SEPolicy, there is a possible way to access the factory MAC address due to a permissions bypass. This could lead to loc

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
Android 14 Security Release Notes   Android Open Source Project	MISC	<a href="https://source.android.com">source.android.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

610548 Google Android March 2024 Security Patch Missing for Huawei EMUI

© 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](#)**