



# CVE-2023-21254

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

## Summary

<b>CVE</b>	CVE-2023-21254
<b>State</b>	PUBLIC
<b>Assigner</b>	security@android.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-13 00:15:00 UTC
<b>Updated</b>	2023-07-25 15:29:00 UTC
<b>Description</b>	In getCurrentState of OneTimePermissionUserManager.java, there is a possible way to hold one-time permissions after the

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
fa539c85503dc63bfb53c76b6f12b3549f14a709 - platform/frameworks/base - Git at Google	MISC	<a href="https://android.googlesource.com">android.googlesource.com</a>	
Android Security Bulletin—July 2023   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>	canor
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canor

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[610494](#) Google Android July 2023 Security Patch Missing for Samsung

[610504](#) Google Android Devices July 2023 Security Patch Missing

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](#)**