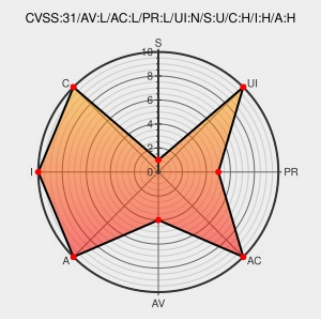
CVE-2023-21374

Published on: Not Yet Published

Last Modified on: 11/04/2023 03:22:00 AM UTC

CVE-2023-21374

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



Certain versions of Android from Google contain the following vulnerability:

In System UI, there is a possible factory reset protection bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

CVE-2023-21374 has been assigned by security@android.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Google** - **Android** version **= 14**

CVSS3 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Android 14 Security Release Notes | Android Open Source Project	source.android.com text/html	MISC source.android.com/docs/security/bulletin/android-14

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	14.0	All	All	All

cpe:2.3:o:google:android:14.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/k12cybersecurity	UPDATED – MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution - PATCH NOW	2023-10-17 15:33:08

← Previous ID

Next ID→