



# CVE-2026-21022

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

## Summary

<b>CVE</b>	CVE-2026-21022
<b>State</b>	PUBLISHED
<b>Assigner</b>	SamsungMobile
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-13 06:16:13 UTC
<b>Updated</b>	2026-05-13 17:26:37 UTC
<b>Description</b>	Improper handling of insufficient permissions in Routines prior to SMR May-2026 Release 1 allows local attackers to access

## Risk And Classification

**Primary CVSS:** v4.0 6.9 MEDIUM from mobile.security@samsung.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000130000 probability, percentile 0.021370000 (date 2026-05-17)

**Problem Types:** NVD-CWE-Other | CWE-280 Improper handling of insufficient permissions or privileges

Version	Source	Type	Score	Severity	Vector
4.0	mobile.security@samsung.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality  
 High  
 Integrity  
 None  
 Availability  
 None  
 Sub Conf.  
 None  
 Sub Integrity  
 None  
 Sub Availability  
 None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSG:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Samsung	Android	15.0	-	All	All
Operating System	Samsung	Android	15.0	smr-apr-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-apr-2026-r1	All	All
Operating System	Samsung	Android	15.0	smr-aug-2025-r1	All	All

Operating System	Samsung	Android	15.0	smr-dec-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-feb-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-feb-2026-r1	All	All
Operating System	Samsung	Android	15.0	smr-jan-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-jan-2026-r1	All	All
Operating System	Samsung	Android	15.0	smr-jul-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-jun-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-mar-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-mar-2026-r1	All	All
Operating System	Samsung	Android	15.0	smr-may-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-nov-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-oct-2025-r1	All	All
Operating System	Samsung	Android	15.0	smr-sep-2025-r1	All	All
Operating System	Samsung	Android	16.0	-	All	All
Operating System	Samsung	Android	16.0	smr-apr-2026-r1	All	All
Operating System	Samsung	Android	16.0	smr-aug-2025-r1	All	All
Operating System	Samsung	Android	16.0	smr-dec-2025-r1	All	All
Operating System	Samsung	Android	16.0	smr-feb-2026-r1	All	All
Operating System	Samsung	Android	16.0	smr-jan-2026-r1	All	All
Operating System	Samsung	Android	16.0	smr-mar-2026-r1	All	All
Operating System	Samsung	Android	16.0	smr-nov-2025-r1	All	All
Operating System	Samsung	Android	16.0	smr-oct-2025-r1	All	All
Operating System	Samsung	Android	16.0	smr-sep-2025-r1	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Samsung Mobile	Samsung Mobile Devices	unaffected SMR May-2026 Release in Android 15, 16 * semver	Not specified

#### References

Reference	Source	Link	Tags
security.samsungmobile.com/securityUpdate.smsb	mobile.security@samsung.com	<a href="https://security.samsungmobile.com">security.samsungmobile.com</a>	Vendor Advisory
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.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)