



CVE-2026-21021

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2026-21021
State	PUBLISHED
Assigner	SamsungMobile
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 06:16:13 UTC
Updated	2026-05-13 17:29:00 UTC
Description	Improper input validation in Routines prior to SMR May-2026 Release 1 allows physical attackers to launch privileged activi

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from mobile.security@samsung.com

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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: 0.000440000 probability, percentile 0.135810000 (date 2026-05-18)

Problem Types: NVD-CWE-noinfo | CWE-20: Improper Input Validation

Version	Source	Type	Score	Severity	Vector
4.0	mobile.security@samsung.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:
3.1	nvd@nist.gov	Primary	6.8	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/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

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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 16 * semver	Not specified

References

Reference	Source	Link	Tags
security.samsungmobile.com/securityUpdate.smsb	mobile.security@samsung.com	security.samsungmobile.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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