



CVE-2026-34849

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

Summary

CVE	CVE-2026-34849
State	PUBLISHED
Assigner	huawei
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 05:16:03 UTC
Updated	2026-04-14 16:34:28 UTC
Description	UAF vulnerability in the screen management module. Impact: Successful exploitation of this vulnerability may affect availab

Risk And Classification

Primary CVSS: v3.1 4.7 MEDIUM from nvd@nist.gov

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

EPSS: 0.000060000 probability, percentile 0.003060000 (date 2026-04-15)

Problem Types: CWE-362 | CWE-362 CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	psirt@huawei.com	Secondary	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Huawei	Harmonyos	5.1.0	All	All	All
Operating System	Huawei	Harmonyos	6.0.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Huawei	HarmonyOS	affected 6.0.0	Not specified
CNA	Huawei	HarmonyOS	affected 5.1.0	Not specified

References

Reference	Source	Link	Tags
consumer.huawei.com/en/support/bulletin/2026/4	psirt@huawei.com	consumer.huawei.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