CVE-2026-41964

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-41964
State	PUBLISHED
Assigner	huawei
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 10:16:35 UTC
Updated	2026-05-15 10:16:35 UTC
Description	Permission control vulnerability in the web. Impact: Successful exploitation of this vulnerability may affect availability.

Risk And Classification

Primary CVSS: v3.1 8.4 HIGH from psirt@huawei.com

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

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	psirt@huawei.com	Secondary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Huawei	HarmonyOS	affected 6.1.0	Not specified
CNA	Huawei	HarmonyOS	affected 6.0.0	Not specified

References

Reference	Source	Link	Tags
consumer.huawei.com/en/support/bulletinlaptops/2026/5	psirt@huawei.com	consumer.huawei.com	
consumer.huawei.com/en/support/bulletin/2026/5	psirt@huawei.com	consumer.huawei.com	
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.