exec: don't WARN for racy path_noexec check

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

Summary

CVE	CVE-2024-50010
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 19:15:04 UTC
Updated	2026-05-12 13:16:15 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: exec: don't WARN for racy path_noexec check Both i_mo

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: 0.000110000 probability, percentile 0.015050000 (date 2026-05-12)

Problem Types: NVD-CWE-noinfo

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	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 0fd338b2d2cdf827091ae819ae90ad760b94ad0c c9b774
CNA	Linux	Linux	affected 0fd338b2d2cdf827091ae819ae90ad760b94ad0c b723f9
CNA	Linux	Linux	affected 0fd338b2d2cdf827091ae819ae90ad760b94ad0c 0bdf77
CNA	Linux	Linux	affected 0fd338b2d2cdf827091ae819ae90ad760b94ad0c 0d16f5
CNA	Linux	Linux	affected 0fd338b2d2cdf827091ae819ae90ad760b94ad0c 0d196e
CNA	Linux	Linux	affected 5.9
CNA	Linux	Linux	unaffected 5.9 semver
CNA	Linux	Linux	unaffected 5.10.229 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.170 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.115 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.59 6.6.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/b723f96407a0a078cf75970e4dbf16b46d286a61	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cor
git.kernel.org/stable/c/0d196e7589cefe207d5d41f37a0a28a1fdeeb7c6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/0bdf77be2330062b3a64f2bec39f62ab874a6796	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/0d16f53c91111cec914f0811fcc526a2ba77b20d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/c9b77438077d5a20c79ead95bcdaf9bd4797baaf	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**