



fs/ntfs3: validate rec->used in journal-replay file record check

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

Summary

CVE	CVE-2026-31716
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:21 UTC
Updated	2026-05-03 07:16:18 UTC

Description In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: validate rec->used in journal-replay file record check

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.048520000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected b46acd6a6a627d876898e1c84d3f84902264b445 f90b8a1798b750755a9e9aee66678f0a1820bbafe git
CNA	Linux	Linux	affected b46acd6a6a627d876898e1c84d3f84902264b445 4b1613d7e2deda831a97e427d1ea586e50fe1be5 g
CNA	Linux	Linux	affected b46acd6a6a627d876898e1c84d3f84902264b445 0112e6279420d4005b3d57af36fb45c01b8d0116 gi
CNA	Linux	Linux	affected b46acd6a6a627d876898e1c84d3f84902264b445 f79d0403ea20a81bc29105bba54fbcab54e8c403 gi
CNA	Linux	Linux	affected b46acd6a6a627d876898e1c84d3f84902264b445 0ca0485e4b2e837ebb6cbd4f2451aba665a03e4b g
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.84 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.25 6.18.* semver
CNA	Linux	Linux	unaffected 7.0.2 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/0ca0485e4b2e837ebb6cbd4f2451aba665a03e4b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f79d0403ea20a81bc29105bba54fbcab54e8c403	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f90b8a1798b750755a9e9aee66678f0a1820bbafe	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0112e6279420d4005b3d57af36fb45c01b8d0116	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/4b1613d7e2deda831a97e427d1ea586e50fe1be5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

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