



smb: client: require a full NFS mode SID before reading mode bits

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

Summary

CVE	CVE-2026-43350
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 14:16:45 UTC
Updated	2026-05-11 08:16:10 UTC

Description In the Linux kernel, the following vulnerability has been resolved: smb: client: require a full NFS mode SID before reading m

Risk And Classification

Primary CVSS: v3.1 7.6 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.049330000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H
3.1	CNA	DECLARED	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected e2f8fbfb8d09c06decde162090fac3ee220aa280 b53b8e98c23310294fc45fc686db5ee860311896 git
CNA	Linux	Linux	affected e2f8fbfb8d09c06decde162090fac3ee220aa280 c8eef12af1cc73031639ea7cf16e0b10e2536b0b git
CNA	Linux	Linux	affected e2f8fbfb8d09c06decde162090fac3ee220aa280 38a69f08ee82c450d3e4168707fff2e317dc3ff7 git
CNA	Linux	Linux	affected e2f8fbfb8d09c06decde162090fac3ee220aa280 f8488c07bea2431ee12a6067d736578064fa46b4 git
CNA	Linux	Linux	affected e2f8fbfb8d09c06decde162090fac3ee220aa280 2757ad3e4b6f9e0fed4c7739594e702abc5cab21 git
CNA	Linux	Linux	affected 5.4
CNA	Linux	Linux	unaffected 5.4 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/c8eef12af1cc73031639ea7cf16e0b10e2536b0b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b53b8e98c23310294fc45fc686db5ee860311896	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/38a69f08ee82c450d3e4168707fff2e317dc3ff7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2757ad3e4b6f9e0fed4c7739594e702abc5cab21	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f8488c07bea2431ee12a6067d736578064fa46b4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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