smb: server: make use of smbdirect_socket.recv_io.credits.available

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

Summary

CVE	CVE-2026-31538
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:27 UTC
Updated	2026-04-28 18:59:51 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: smb: server: make use of smbdirect_socket.recv_io.credit

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000170000 probability, percentile 0.040590000 (date 2026-04-27)

Problem Types: NVD-CWE-Other

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

vailability

High

CVSS:3.1/AV:N/AC:L/PR:N/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 89b021a72663c4d96d8a8b85272bb42d991a1c6f 66c082e3d4651e8629a393a9e182b01eb50fb0a3 g
CNA	Linux	Linux	affected 89b021a72663c4d96d8a8b85272bb42d991a1c6f 809cbd31aa4f87a1b889532244c9cf30eb022385 gi
CNA	Linux	Linux	affected 89b021a72663c4d96d8a8b85272bb42d991a1c6f 26ad87a2cfb8c1384620d1693a166ed87303046e g
CNA	Linux	Linux	affected 6.18
CNA	Linux	Linux	unaffected 6.18 semver
CNA	Linux	Linux	unaffected 6.18.11 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.1 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/66c082e3d4651e8629a393a9e182b01eb50fb0a3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/809cbd31aa4f87a1b889532244c9cf30eb022385	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/26ad87a2cfb8c1384620d1693a166ed87303046e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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.

Free CVE JSON API cve.report/api

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