smb: client: fix OOB read in smb2_ioctl_query_info QUERY_INFO path

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

Summary

CVE	CVE-2026-31708
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:20 UTC
Updated	2026-05-03 07:16:18 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix OOB read in smb2_ioctl_query_info QUER

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/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	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H
3.1	CNA	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Unchanged

Confidentiality
High

Integrity
None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected f5778c398713692a16150ae96e5c8270bab8399f a34d456934fe42e4da5d2cc07787bf418bee99c6 git
CNA	Linux	Linux	affected f5778c398713692a16150ae96e5c8270bab8399f ac2f14e4705d020f04e806efa0d49ab8dc2b145f git
CNA	Linux	Linux	affected f5778c398713692a16150ae96e5c8270bab8399f 078fae8f50adebb903ccf2252b44391324571e78 git
CNA	Linux	Linux	affected f5778c398713692a16150ae96e5c8270bab8399f 85fd46ee26a11841c670449508025965f61ce131 git
CNA	Linux	Linux	affected f5778c398713692a16150ae96e5c8270bab8399f a58c5af19ff0d6f44f6e9fe31e33a2c92223f77e git
CNA	Linux	Linux	affected 5.1
CNA	Linux	Linux	unaffected 5.1 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/ac2f14e4705d020f04e806efa0d49ab8dc2b145f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/85fd46ee26a11841c670449508025965f61ce131	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/078fae8f50adebb903ccf2252b44391324571e78	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a34d456934fe42e4da5d2cc07787bf418bee99c6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a58c5af19ff0d6f44f6e9fe31e33a2c92223f77e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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