ksmbd: fix mechToken leak when SPNEGO decode fails after token alloc

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

Summary

CVE	CVE-2026-31610
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:40 UTC
Updated	2026-04-29 16:51:02 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix mechToken leak when SPNEGO decode fails a

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000340000 probability, percentile 0.098310000 (date 2026-04-27)

Problem Types: CWE-401

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity
None

Availability
High

CVSS:3.1/AV:L/AC:L/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 fad4161b5cd01a24202234976ebbb133f7adc0b5 745a535461bbb90a56d9357573c9f97a5c12abe1 gi
CNA	Linux	Linux	affected fad4161b5cd01a24202234976ebbb133f7adc0b5 dd577cb55588ec3fbc66af3621280306601c4192 git
CNA	Linux	Linux	affected fad4161b5cd01a24202234976ebbb133f7adc0b5 dd53414e301beb915fe672dc4c4a51bafb917604 git
CNA	Linux	Linux	affected fad4161b5cd01a24202234976ebbb133f7adc0b5 269c800a7a7e363459291885b35f7bc72e231ed6 gi
CNA	Linux	Linux	affected fad4161b5cd01a24202234976ebbb133f7adc0b5 6c8c44e6553b9f072f62d9875e567766eb293162 git
CNA	Linux	Linux	affected fad4161b5cd01a24202234976ebbb133f7adc0b5 ad0057fb91218914d6c98268718ceb9d59b388e1 gi
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 6.12.83 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.24 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.14 6.19.* semver
CNA	Linux	Linux	unaffected 7.0.1 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/ad0057fb91218914d6c98268718ceb9d59b388e1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/745a535461bbb90a56d9357573c9f97a5c12abe1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/269c800a7a7e363459291885b35f7bc72e231ed6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/dd577cb55588ec3fbc66af3621280306601c4192	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/6c8c44e6553b9f072f62d9875e567766eb293162	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/dd53414e301beb915fe672dc4c4a51bafb917604	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