procfs: fix possible double mmput() in do_procmap_query()

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

Summary

CVE	CVE-2026-43178
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:36 UTC
Updated	2026-05-12 19:52:25 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: procfs: fix possible double mmput() in do_procmap_query

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.000130000 probability, percentile 0.023990000 (date 2026-05-12)

Problem Types: CWE-415

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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 b9b97e6aeb534315f9646b2090d1a5024c6a4e82 f9fe092084cd04deea18747f58a2304026e76aaa git
CNA	Linux	Linux	affected cbc03ce3e6ce7e21214c3f02218213574c1a2d08 8adaff87db143583e08eec4f4e7788f1ef8af94d git
CNA	Linux	Linux	affected b5cbacd7f86f4f62b8813688c8e73be94e8e1951 90f5e87c9b75833b9ef3a4415b92c0247f28ab2f git
CNA	Linux	Linux	affected b5cbacd7f86f4f62b8813688c8e73be94e8e1951 61dc9f776705d6db6847c101b98fa4f0e9eb6fa3 git
CNA	Linux	Linux	affected 6.19
CNA	Linux	Linux	unaffected 6.19 semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/90f5e87c9b75833b9ef3a4415b92c0247f28ab2f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f9fe092084cd04deea18747f58a2304026e76aaa	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8adaff87db143583e08eec4f4e7788f1ef8af94d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/61dc9f776705d6db6847c101b98fa4f0e9eb6fa3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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.