mm/vma: fix anon_vma UAF on mremap() faulted, unfaulted merge

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-23077
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-04 17:16:18 UTC
Updated	2026-04-03 14:16:22 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: mm/vma: fix anon_vma UAF on mremap() faulted, unfault

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: 0.000170000 probability, percentile 0.039420000 (date 2026-04-03)

Problem Types: CWE-416

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
Operating System	Linux	Linux Kernel	6.19	rc1	All	All
Operating System	Linux	Linux Kernel	6.19	rc2	All	All
Operating System	Linux	Linux Kernel	6.19	rc3	All	All
Operating System	Linux	Linux Kernel	6.19	rc4	All	All
Operating System	Linux	Linux Kernel	6.19	rc5	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 879bca0a2c4f40b08d09a95a2a0c3c6513060b5c a4d9dbfc1bab16e25fefd34b5e537a46bed8fc96 git
CNA	Linux	Linux	affected 879bca0a2c4f40b08d09a95a2a0c3c6513060b5c 61f67c230a5e7c741c352349ea80147fbe65bfae git
CNA	Linux	Linux	affected 6.16
CNA	Linux	Linux	unaffected 6.16 semver
CNA	Linux	Linux	unaffected 6.18.8 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/a4d9dbfc1bab16e25fefd34b5e537a46bed8fc96	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/61f67c230a5e7c741c352349ea80147fbe65bfae	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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.