mshv: Fix use-after-free in mshv_map_user_memory error path

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

Summary

CVE	CVE-2026-23432
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 16:16:24 UTC
Updated	2026-04-23 21:00:48 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: mshv: Fix use-after-free in mshv_map_user_memory erro

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: 0.000150000 probability, percentile 0.028630000 (date 2026-04-24)

Problem Types: CWE-416

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

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	-	All	All
Operating System	Linux	Linux Kernel	7.0	rc1	All	All
Operating System	Linux	Linux Kernel	7.0	rc2	All	All
Operating System	Linux	Linux Kernel	7.0	rc3	All	All
Operating System	Linux	Linux Kernel	7.0	rc4	All	All
Operating System	Linux	Linux Kernel	7.0	rc5	All	All
Operating System	Linux	Linux Kernel	7.0	rc6	All	All
Operating System	Linux	Linux Kernel	7.0	rc7	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected b9a66cd5ccbb9fade15d0e427e19470d8ad35b75 34861bdc0c0196b6c2dd48f7454029407704ff6e git
CNA	Linux	Linux	affected b9a66cd5ccbb9fade15d0e427e19470d8ad35b75 6922db250422a0dfee34de322f86b7a73d713d33 gi
CNA	Linux	Linux	affected 6.19
CNA	Linux	Linux	unaffected 6.19 semver
CNA	Linux	Linux	unaffected 6.19.10 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/34861bdc0c0196b6c2dd48f7454029407704ff6e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/6922db250422a0dfee34de322f86b7a73d713d33	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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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