



mm: call the security_mmap_file() LSM hook in remap_file_pages()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2024-47745
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 13:15:04 UTC
Updated	2026-05-12 19:07:20 UTC

Description In the Linux kernel, the following vulnerability has been resolved: mm: call the security_mmap_file() LSM hook in remap_file

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

Problem Types: CWE-670

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	Debian	Debian Linux	11.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected c8d78c1823f46519473949d33f0d1d33fe21ea16 0f910dbf2f2a4a7820ba4bac7b280f7108aa05b1 git
CNA	Linux	Linux	affected c8d78c1823f46519473949d33f0d1d33fe21ea16 49d3a4ad57c57227c3b0fd6cd4188b2a5ebd6178 git
CNA	Linux	Linux	affected c8d78c1823f46519473949d33f0d1d33fe21ea16 3393fddbfa947c8e1fdcc4509226905ffffd8b89 git
CNA	Linux	Linux	affected c8d78c1823f46519473949d33f0d1d33fe21ea16 ce14f38d6ee9e88e37ec28427b4b93a7c33c70d3 git
CNA	Linux	Linux	affected c8d78c1823f46519473949d33f0d1d33fe21ea16 ea7e2d5e49c05e5db1922387b09ca74aa40f46e2 git
CNA	Linux	Linux	affected 097f98edde717ce09f217d8a285fe357dcd29fd1 git
CNA	Linux	Linux	affected 4.0
CNA	Linux	Linux	unaffected 4.0 semver
CNA	Linux	Linux	unaffected 6.1.120 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.54 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.13 6.10.* semver
CNA	Linux	Linux	unaffected 6.11.2 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/ce14f38d6ee9e88e37ec28427b4b93a7c33c70d3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/ea7e2d5e49c05e5db1922387b09ca74aa40f46e2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/49d3a4ad57c57227c3b0fd6cd4188b2a5ebd6178	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
lists.debian.org/debian-lts-announce/2025/03/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Maili
git.kernel.org/stable/c/0f910dbf2f2a4a7820ba4bac7b280f7108aa05b1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/3393fddbfa947c8e1fdcc4509226905ffffd8b89	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

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 registered 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](#)