dma-buf: heaps: Fix off-by-one in CMA heap fault handler

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

Summary

CVE	CVE-2024-46852
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-09-27 13:15:16 UTC
Updated	2026-05-05 15:20:17 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: dma-buf: heaps: Fix off-by-one in CMA heap fault handler

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-193

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 a5d2d29e24be8967ef78a1b1fb2292413e3b3df9 79cce5e81d20fa9ad553be439d665ac3302d3c95 git
CNA	Linux	Linux	affected a5d2d29e24be8967ef78a1b1fb2292413e3b3df9 84175dc5b2c932266a50c04e5ce342c30f817a2f git
CNA	Linux	Linux	affected a5d2d29e24be8967ef78a1b1fb2292413e3b3df9 eb7fc8b65cea22f9038c52398c8b22849e9620ea git
CNA	Linux	Linux	affected a5d2d29e24be8967ef78a1b1fb2292413e3b3df9 e79050882b857c37634baedbdcf7c2047c24cbff git
CNA	Linux	Linux	affected a5d2d29e24be8967ef78a1b1fb2292413e3b3df9 ea5ff5d351b520524019f7ff7f9ce418de2dad87 git
CNA	Linux	Linux	affected 5.11
CNA	Linux	Linux	unaffected 5.11 semver
CNA	Linux	Linux	unaffected 5.15.168 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.111 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.52 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.11 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/79cce5e81d20fa9ad553be439d665ac3302d3c95	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/e79050882b857c37634baedbdcf7c2047c24cbff	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/eb7fc8b65cea22f9038c52398c8b22849e9620ea	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/84175dc5b2c932266a50c04e5ce342c30f817a2f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Maili
git.kernel.org/stable/c/ea5ff5d351b520524019f7ff7f9ce418de2dad87	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

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