tracing/dma: Cap dma_map_sg tracepoint arrays to prevent buffer overflow

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

Summary

CVE	CVE-2026-23390
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:39 UTC
Updated	2026-04-24 18:32:24 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: tracing/dma: Cap dma_map_sg tracepoint arrays to preve

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-787

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 038eb433dc1474c4bc7d33188294e3d4778efdfd 02d209bb018a40dee9eac89e91860253dee9605b g
CNA	Linux	Linux	affected 038eb433dc1474c4bc7d33188294e3d4778efdfd f2584f791a10343bdc995ff6ff402db45b95de69 git
CNA	Linux	Linux	affected 038eb433dc1474c4bc7d33188294e3d4778efdfd daafcc0ef0b358d9d622b6e3b7c43767aa3814ee git
CNA	Linux	Linux	affected 6.12
CNA	Linux	Linux	unaffected 6.12 semver
CNA	Linux	Linux	unaffected 6.12.74 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.13 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/f2584f791a10343bdc995ff6ff402db45b95de69	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/02d209bb018a40dee9eac89e91860253dee9605b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/daafcc0ef0b358d9d622b6e3b7c43767aa3814ee	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.