



# tracing/dma: Cap dma\_map\_sg tracepoint arrays to prevent buffer overflow

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

## Summary

<b>CVE</b>	CVE-2026-23390
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 11:16:39 UTC
<b>Updated</b>	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	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 038eb433dc1474c4bc7d33188294e3d4778efdfd 02d209bb018a40dee9eac89e91860253dee9605b g
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 038eb433dc1474c4bc7d33188294e3d4778efdfd f2584f791a10343bdc995ff6ff402db45b95de69 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 038eb433dc1474c4bc7d33188294e3d4778efdfd daafcc0ef0b358d9d622b6e3b7c43767aa3814ee git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.12
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.74 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.13 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19 * original_commit_for_fix

## References

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

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)