



# mm/damon/sysfs: check contexts->nr before accessing contexts\_arr[0]

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

## Summary

<b>CVE</b>	CVE-2026-31458
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-22 14:16:41 UTC
<b>Updated</b>	2026-04-22 14:16:41 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: mm/damon/sysfs: check contexts->nr before accessing cc

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0ac32b8affb5a384253dbb8339bd2d0e91add0b7_aba546061341b56e9ffb37e1eb661a3628b6ec12 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0ac32b8affb5a384253dbb8339bd2d0e91add0b7_1e8da792672481d603fa7cd0d815577220a3ee27 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0ac32b8affb5a384253dbb8339bd2d0e91add0b7_708033c231bd782858f4ddb46ee874a5a5fbdab git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0ac32b8affb5a384253dbb8339bd2d0e91add0b7_bbe03ad3fb9e714191757ca7b41582f930be7be2 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0ac32b8affb5a384253dbb8339bd2d0e91add0b7_1bfe9fb5ed2667fb075682408b776b5273162615 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 5.18
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.18 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.131 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.80 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.21 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.11 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/708033c231bd782858f4ddb46ee874a5a5fbdab	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/1bfe9fb5ed2667fb075682408b776b5273162615	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/aba546061341b56e9ffb37e1eb661a3628b6ec12	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	
git.kernel.org/stable/c/1e8da792672481d603fa7cd0d815577220a3ee27	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="#">git.kernel.org</a>	

git.kernel.org/stable/c/bbe03ad3fb9e714191757ca7b41582f930be7be2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**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)