



# RDMA/umem: Fix double dma\_buf\_unpin in failure path

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

## Summary

|                        |                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2026-43128                                                                                                             |
| <b>State</b>           | PUBLISHED                                                                                                                  |
| <b>Assigner</b>        | Linux                                                                                                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                               |
| <b>Published</b>       | 2026-05-06 12:16:29 UTC                                                                                                    |
| <b>Updated</b>         | 2026-05-08 17:52:13 UTC                                                                                                    |
| <b>Description</b>     | In the Linux kernel, the following vulnerability has been resolved: RDMA/umem: Fix double dma_buf_unpin in failure path In |

## 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

**EPSS:** 0.000130000 probability, percentile 0.024500000 (date 2026-05-12)

**Problem Types:** CWE-415

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | nvd@nist.gov                         | Primary   | 7.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1     | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | Secondary | 7.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1     | CNA                                  | DECLARED  | 7.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |

## 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 1e4df4a21c5ac722df1099eee30cad9246c889b5 70542b69abff34d24b11ae0bb200cc7a766d18df git |
| CNA                               | Linux  | Linux   | affected 1e4df4a21c5ac722df1099eee30cad9246c889b5 b324327ff6f48d8065dca67eb3b91357e72726bd git |
| CNA                               | Linux  | Linux   | affected 1e4df4a21c5ac722df1099eee30cad9246c889b5 ba3bf0f1bf1d5d0404678485e872980532fcc2c4 git |
| CNA                               | Linux  | Linux   | affected 1e4df4a21c5ac722df1099eee30cad9246c889b5 d3e32e2f3262f1b25d77c085ace38e2cc4ad75cf git |
| CNA                               | Linux  | Linux   | affected 1e4df4a21c5ac722df1099eee30cad9246c889b5 40126bcbefa79ea86672e05dae608596bab38319 gi  |
| CNA                               | Linux  | Linux   | affected 1e4df4a21c5ac722df1099eee30cad9246c889b5 104016eb671e19709721c1b0048dd912dc2e96be g   |
| CNA                               | Linux  | Linux   | affected 5.16                                                                                  |
| CNA                               | Linux  | Linux   | unaffected 5.16 semver                                                                         |
| CNA                               | Linux  | Linux   | unaffected 6.1.165 6.1.* semver                                                                |
| CNA                               | Linux  | Linux   | unaffected 6.6.128 6.6.* semver                                                                |
| CNA                               | Linux  | Linux   | unaffected 6.12.75 6.12.* semver                                                               |
| CNA                               | Linux  | Linux   | unaffected 6.18.16 6.18.* semver                                                               |
| CNA                               | Linux  | Linux   | unaffected 6.19.6 6.19.* semver                                                                |
| CNA                               | Linux  | Linux   | unaffected 7.0 * original_commit_for_fix                                                       |



| References                                                       |                                      |                |         |
|------------------------------------------------------------------|--------------------------------------|----------------|---------|
| Reference                                                        | Source                               | Link           | Tags    |
| git.kernel.org/stable/c/d3e32e2f3262f1b25d77c085ace38e2cc4ad75cf | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch   |
| git.kernel.org/stable/c/104016eb671e19709721c1b0048dd912dc2e96be | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch   |
| git.kernel.org/stable/c/70542b69abff34d24b11ae0bb200cc7a766d18df | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch   |
| git.kernel.org/stable/c/ba3bf0f1bf1d5d0404678485e872980532fcc2c4 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch   |
| git.kernel.org/stable/c/40126bcbefa79ea86672e05dae608596bab38319 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Patch   |
| git.kernel.org/stable/c/b324327ff6f48d8065dca67eb3b91357e72726bd | 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.

© [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](#)