



# nvmem: zynqmp\_nvmem: Fix buffer size in DMA and memcpy

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

## Summary

|                        |                                              |
|------------------------|----------------------------------------------|
| <b>CVE</b>             | CVE-2026-31743                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Linux                                        |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-05-01 15:16:37 UTC                      |
| <b>Updated</b>         | 2026-05-03 07:16:19 UTC                      |

**Description** In the Linux kernel, the following vulnerability has been resolved: nvmem: zynqmp\_nvmem: Fix buffer size in DMA and men

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

**CVSS:** 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.000180000 probability, percentile 0.046600000 (date 2026-05-02)

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|----------------------------------------------|
| 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

### Vendor Declared Affected Products

| Source | Vendor | Product | Version                                                                                        |
|--------|--------|---------|------------------------------------------------------------------------------------------------|
| CNA    | Linux  | Linux   | affected 737c0c8d07b5f671c0a33cec95965fcb2d2ea893 2f6e5b9964d0a63a5ba84fca2642876afb70a662 git |
| CNA    | Linux  | Linux   | affected 737c0c8d07b5f671c0a33cec95965fcb2d2ea893 784ed4abded1ca4b525fa4cade8b02f8c5d2a087 git |
| CNA    | Linux  | Linux   | affected 737c0c8d07b5f671c0a33cec95965fcb2d2ea893 6c01e7f11f5e5f22285d19510a9643e2506e13c3 git |
| CNA    | Linux  | Linux   | affected 737c0c8d07b5f671c0a33cec95965fcb2d2ea893 f9b88613ff402aa6fe8fd020573cb95867ae947e git |
| CNA    | Linux  | Linux   | affected 6.9                                                                                   |
| CNA    | Linux  | Linux   | unaffected 6.9 semver                                                                          |
| CNA    | Linux  | Linux   | unaffected 6.12.81 6.12.* semver                                                               |
| CNA    | Linux  | Linux   | unaffected 6.18.22 6.18.* semver                                                               |
| CNA    | Linux  | Linux   | unaffected 6.19.12 6.19.* semver                                                               |
| CNA    | Linux  | Linux   | unaffected 7.0 * original_commit_for_fix                                                       |

### References

| Reference                                                        | Source                               | Link                                                | Tags      |
|------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------|-----------|
| git.kernel.org/stable/c/f9b88613ff402aa6fe8fd020573cb95867ae947e | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| git.kernel.org/stable/c/784ed4abded1ca4b525fa4cade8b02f8c5d2a087 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| git.kernel.org/stable/c/6c01e7f11f5e5f22285d19510a9643e2506e13c3 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| git.kernel.org/stable/c/2f6e5b9964d0a63a5ba84fca2642876afb70a662 | 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>       | canonical |
| NVD vulnerability detail                                         | NVD                                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     | canonical |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web](https://cve.mitre.org)

[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)