



# drm/amdgpu: add upper bound check on user inputs in signal ioctl

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-43400                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Linux  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-05-08 15:16:51 UTC                      |
| <b>Updated</b>         | 2026-05-12 14:10:27 UTC                      |

**Description** In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: add upper bound check on user inputs in signal ioctl

## Risk And Classification

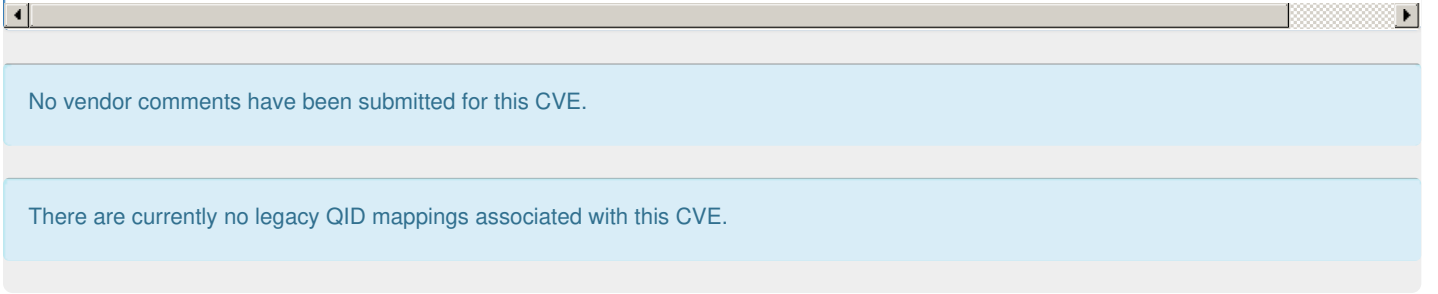
**EPSS:** 0.000170000 probability, percentile 0.041320000 (date 2026-05-12)

## Vendor Declared Affected Products

| Source | Vendor                | Product               | Version  |
|--------|-----------------------|-----------------------|--|
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected a292fdecd72834b3bec380baa5db1e69e7f70679 6fff5204d8aa26b1be50b6427f833bd3e8899c4f git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected a292fdecd72834b3bec380baa5db1e69e7f70679 46630d966b99b0fc6cb01fef4110587f3375a0c0 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected a292fdecd72834b3bec380baa5db1e69e7f70679 ea78f8c68f4f6211c557df49174c54d167821962 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 6.16  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.16 semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.18.19 6.18.* semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.19.9 6.19.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 7.0 * original_commit_for_fix   |

## References

| Reference   | Source                               | Link  | Tags      |
|---|--------------------------------------|---|-----------|
| <a href="https://git.kernel.org/stable/c/46630d966b99b0fc6cb01fef4110587f3375a0c0">git.kernel.org/stable/c/46630d966b99b0fc6cb01fef4110587f3375a0c0</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/ea78f8c68f4f6211c557df49174c54d167821962">git.kernel.org/stable/c/ea78f8c68f4f6211c557df49174c54d167821962</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/6fff5204d8aa26b1be50b6427f833bd3e8899c4f">git.kernel.org/stable/c/6fff5204d8aa26b1be50b6427f833bd3e8899c4f</a> | 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](#) 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](#)