



# media: chips-media: wave5: Fix SError of kernel panic when closed

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-43247                               |
| <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 12:16:45 UTC                      |
| <b>Updated</b>         | 2026-05-06 13:07:51 UTC                      |

**Description** In the Linux kernel, the following vulnerability has been resolved: media: chips-media: wave5: Fix SError of kernel panic wh

## Vendor Declared Affected Products

| Source | Vendor                | Product               | Version  |
|--------|-----------------------|-----------------------|--|
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 2092b3833487e5ce138f4303f98e46ba0f87f1d0 27cb12b7dc88c51582094eeb2b65b0e94603e411 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 2092b3833487e5ce138f4303f98e46ba0f87f1d0 5da55243fe190c2165ed34e77091a43c0ff74f10 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 2092b3833487e5ce138f4303f98e46ba0f87f1d0 cbb9c0d50e471483cced55f5b7db4569dcd959a6 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 6.13  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.13 semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.18.16 6.18.* semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.19.6 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/cbb9c0d50e471483cced55f5b7db4569dcd959a6">git.kernel.org/stable/c/cbb9c0d50e471483cced55f5b7db4569dcd959a6</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/5da55243fe190c2165ed34e77091a43c0ff74f10">git.kernel.org/stable/c/5da55243fe190c2165ed34e77091a43c0ff74f10</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |         |
| <a href="https://git.kernel.org/stable/c/27cb12b7dc88c51582094eeb2b65b0e94603e411">git.kernel.org/stable/c/27cb12b7dc88c51582094eeb2b65b0e94603e411</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>       | 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)