



media: mediatek: vcodec: fix use-after-free in encoder release path

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-31584 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-24 15:16:33 UTC |
| Updated | 2026-04-24 17:51:40 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: media: mediatek: vcodec: fix use-after-free in encoder release path

Risk And Classification

EPSS: 0.000180000 probability, percentile 0.046210000 (date 2026-04-25)

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|-----------------------|-----------------------|--|
| CNA | Linux | Linux | affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 a8a55913552aed45108525d1851c65e1db0cc25b git |
| CNA | Linux | Linux | affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 f99353cd0e9f58bf17889049137b8d65fb44ebf1 git |
| CNA | Linux | Linux | affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 93d9a58961a9e09306857e999b3ee76aa4be67f0 git |
| CNA | Linux | Linux | affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 f1692337c6fa26e04f89b22a4d84bf5b7ada50d1 git |
| CNA | Linux | Linux | unaffected 6.12.83 6.12.* semver |
| CNA | Linux | Linux | unaffected 6.18.24 6.18.* semver |
| CNA | Linux | Linux | unaffected 6.19.14 6.19.* semver |
| CNA | Linux | Linux | unaffected 7.0.1 7.0.* semver |

References

| Reference | Source | Link | Tags |
|--|--------------------------------------|--------------------------------|---------|
| git.kernel.org/stable/c/a8a55913552aed45108525d1851c65e1db0cc25b | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/f1692337c6fa26e04f89b22a4d84bf5b7ada50d1 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/93d9a58961a9e09306857e999b3ee76aa4be67f0 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/f99353cd0e9f58bf17889049137b8d65fb44ebf1 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonic |

| | | | |
|--------------------------|---------|--|-----------|
| CVE Program Home | CVE IDs | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | 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