



# spi: spi-fsl-lpspi: fix teardown order issue (UAF)

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-31485                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Linux  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-04-22 14:16:45 UTC                      |
| <b>Updated</b>         | 2026-04-22 14:16:45 UTC                      |

**Description** In the Linux kernel, the following vulnerability has been resolved: spi: spi-fsl-lpspi: fix teardown order issue (UAF) There is a

## Vendor Declared Affected Products

| Source | Vendor | Product | Version  |
|--------|--------|---------|--|
| CNA    | Linux  | Linux   | affected 5314987de5e5f5e38436ef4a69328bc472bbd63e fbe6f40caeebb0b1ea9dfedc259124c1d3cda7a6 git |
| CNA    | Linux  | Linux   | affected 5314987de5e5f5e38436ef4a69328bc472bbd63e ca4483f36ac1b62e69f8b182c5b8f059e0abecfb git |
| CNA    | Linux  | Linux   | affected 5314987de5e5f5e38436ef4a69328bc472bbd63e e3fd54f8b0317fbccc103961ddd660f2a32dcf0b git |
| CNA    | Linux  | Linux   | affected 5314987de5e5f5e38436ef4a69328bc472bbd63e adb25339b66112393fd6892ceff926765feb5b86 git |
| CNA    | Linux  | Linux   | affected 5314987de5e5f5e38436ef4a69328bc472bbd63e d5d01f24bc6fbde40b4e567ef9160194b61267bc git |
| CNA    | Linux  | Linux   | affected 5314987de5e5f5e38436ef4a69328bc472bbd63e e89e2b97253c124d37bf88e96e5e8ce5c3aeec3 gi   |
| CNA    | Linux  | Linux   | affected 5314987de5e5f5e38436ef4a69328bc472bbd63e 15650dfbaeeb14bcaaf053b93cf631db8d465300 git |
| CNA    | Linux  | Linux   | affected 5314987de5e5f5e38436ef4a69328bc472bbd63e b341c1176f2e001b3adf0b47154fc31589f7410e git |
| CNA    | Linux  | Linux   | affected 4.10  |
| CNA    | Linux  | Linux   | unaffected 4.10 semver   |
| CNA    | Linux  | Linux   | unaffected 5.10.253 5.10.* semver  |
| CNA    | Linux  | Linux   | unaffected 5.15.203 5.15.* semver  |
| CNA    | Linux  | Linux   | unaffected 6.1.168 6.1.* semver  |
| CNA    | Linux  | Linux   | unaffected 6.6.131 6.6.* semver  |
| CNA    | Linux  | Linux   | unaffected 6.12.80 6.12.* semver   |
| CNA    | Linux  | Linux   | unaffected 6.18.21 6.18.* semver   |
| CNA    | Linux  | Linux   | unaffected 6.19.11 6.19.* semver   |
| CNA    | Linux  | Linux   | unaffected 7.0 * original_commit_for_fix   |

## References

| Reference   | Source                               | Link  | Tags      |
|---|--------------------------------------|---|-----------|
| <a href="https://git.kernel.org/stable/c/e89e2b97253c124d37bf88e96e5e8ce5c3aeec3">git.kernel.org/stable/c/e89e2b97253c124d37bf88e96e5e8ce5c3aeec3</a>   | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/b341c1176f2e001b3adf0b47154fc31589f7410e">git.kernel.org/stable/c/b341c1176f2e001b3adf0b47154fc31589f7410e</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/ca4483f36ac1b62e69f8b182c5b8f059e0abecfb">git.kernel.org/stable/c/ca4483f36ac1b62e69f8b182c5b8f059e0abecfb</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/e3fd54f8b0317fbccc103961ddd660f2a32dcf0b">git.kernel.org/stable/c/e3fd54f8b0317fbccc103961ddd660f2a32dcf0b</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/fbe6f40caeabb0b1ea9dfedc259124c1d3cda7a6">git.kernel.org/stable/c/fbe6f40caeabb0b1ea9dfedc259124c1d3cda7a6</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/d5d01f24bc6fbde40b4e567ef9160194b61267bc">git.kernel.org/stable/c/d5d01f24bc6fbde40b4e567ef9160194b61267bc</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/15650dfbaeeb14bcaaf053b93cf631db8d465300">git.kernel.org/stable/c/15650dfbaeeb14bcaaf053b93cf631db8d465300</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/adb25339b66112393fd6892ceff926765feb5b86">git.kernel.org/stable/c/adb25339b66112393fd6892ceff926765feb5b86</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](https://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 site](https://www.mitre.org/cve). 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)