



# f2fs: fix to detect potential corrupted nid in free\_nid\_list

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

## Summary

|                        |                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2025-68315                                                                                                                      |
| <b>State</b>           | PUBLISHED                                                                                                                           |
| <b>Assigner</b>        | Linux                                                                                                                               |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                        |
| <b>Published</b>       | 2025-12-16 16:16:11 UTC                                                                                                             |
| <b>Updated</b>         | 2026-05-17 16:16:14 UTC                                                                                                             |
| <b>Description</b>     | In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to detect potential corrupted nid in free_nid_list As |

## Risk And Classification

**EPSS:** 0.000200000 probability, percentile 0.057690000 (date 2026-05-17)

## Vendor Declared Affected Products

| Source | Vendor                | Product               | Version                                                                                        |
|--------|-----------------------|-----------------------|------------------------------------------------------------------------------------------------|
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 9337ed5e777e1c19854928cba7a8131dd00e611b c   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 6b9525596a83cd5b7bbc2c7bd5f9ad9cf5ad60fa git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 adbc34f03abb89e681a5907c4c3ce4bf224991d git  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 8fc6056dcf79937c46c97fa4996cda65956437a9 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 3.8                                                                                   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 3.8 semver                                                                          |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.6.140 6.6.* semver                                                                |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.12.58 6.12.* semver                                                               |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.17.8 6.17.* semver                                                                |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.18 * original_commit_for_fix                                                      |

## References

| Reference                                                        | Source                               | Link                           | Tags |
|------------------------------------------------------------------|--------------------------------------|--------------------------------|------|
| git.kernel.org/stable/c/9337ed5e777e1c19854928cba7a8131dd00e611b | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="#">git.kernel.org</a> |      |
| git.kernel.org/stable/c/8fc6056dcf79937c46c97fa4996cda65956437a9 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="#">git.kernel.org</a> |      |
| git.kernel.org/stable/c/6b9525596a83cd5b7bbc2c7bd5f9ad9cf5ad60fa | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="#">git.kernel.org</a> |      |
| git.kernel.org/stable/c/adbc34f03abb89e681a5907c4c3ce4bf224991d  | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="#">git.kernel.org</a> |      |

|                          |         |                                                |         |
|--------------------------|---------|------------------------------------------------|---------|
| CVE Program record       | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>   | canonic |
| NVD vulnerability detail | NVD     | <a href="http://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](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)