



f2fs: fix to do sanity check on ino and xnid

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-38347 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-07-10 09:15:29 UTC |
| Updated | 2026-05-12 13:16:48 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on ino and xnid syzbot reported

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: NVD-CWE-noinfo

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS: 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|--------------|---------|--------|---------|----------|
| Operating System | Linux | Linux Kernel | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|---------|-----------------|--|
| CNA | Linux | Linux | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 44e904a1ad09e84039058dcbbb1b9ea5f |
| CNA | Linux | Linux | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 ecff54aa20b5b21db82e63e46066b55e4f |
| CNA | Linux | Linux | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 c4029044cc408b149e63db7dc8617a07f |
| CNA | Linux | Linux | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 e98dc1909f3d5bc078ec7a605524f1e3f4 |
| CNA | Linux | Linux | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 aaddc6c696bd1bff20eaacfa88579d6eae |
| CNA | Linux | Linux | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 fed611bd8c7b76b070aa407d0c7558e20 |
| CNA | Linux | Linux | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 5a06d97d5340c00510f24e80e8de821bc |
| CNA | Linux | Linux | affected 98e4da8ca301e062d79ae168c67e56f3c3de3ce4 061cf3a84bde038708eb0f1d065b31b7c |
| CNA | Linux | Linux | affected 3.8 |
| CNA | Linux | Linux | unaffected 3.8 semver |
| CNA | Linux | Linux | unaffected 5.4.297 5.4.* semver |
| CNA | Linux | Linux | unaffected 5.10.241 5.10.* semver |
| CNA | Linux | Linux | unaffected 5.15.190 5.15.* semver |
| CNA | Linux | Linux | unaffected 6.1.149 6.1.* semver |
| CNA | Linux | Linux | unaffected 6.6.95 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.12.35 6.12.* semver |
| CNA | Linux | Linux | unaffected 6.15.4 6.15.* semver |
| CNA | Linux | Linux | unaffected 6.16 * original_commit_for_fix |
| ADP | Siemens | SIMATIC CN 4100 | affected V5.0 custom |

References

| Reference | Source | Link |
|--|--------------------------------------|--|
| lists.debian.org/debian-lts-announce/2025/10/msg00008.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| git.kernel.org/stable/c/c4029044cc408b149e63db7dc8617a0783a3f10d | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/e98dc1909f3d5bc078ec7a605524f1e3f4c0eb14 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/5a06d97d5340c00510f24e80e8de821bd3bd9285 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| cert-portal.siemens.com/productcert/html/ssa-032379.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com |
| git.kernel.org/stable/c/061cf3a84bde038708eb0f1d065b31b7c2456533 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/fed611bd8c7b76b070aa407d0c7558e20d9e1f68 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/44e904a1ad09e84039058dcbbb1b9ea5b8d7d75d | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |

| | | |
|---|--------------------------------------|---|
| lists.debian.org/debian-lts-announce/2025/10/msg00007.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| git.kernel.org/stable/c/aaddc6c696bd1bff20eaacfa88579d6eae64d541 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/ecff54aa20b5b21db82e63e46066b55e43d72e78 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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