



# io: imu: adis: Fix NULL pointer dereference in adis\_init

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-43356  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | Linux   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-05-08 15:16:46 UTC   |
| <b>Updated</b>         | 2026-05-08 15:16:46 UTC   |
| <b>Description</b>     | In the Linux kernel, the following vulnerability has been resolved: io: imu: adis: Fix NULL pointer dereference in adis_init Th |

## Risk And Classification

**EPSS:** 0.000170000 probability, percentile 0.041270000 (date 2026-05-09)

## Vendor Declared Affected Products

| Source | Vendor                | Product               | Version  |
|--------|-----------------------|-----------------------|--|
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 3b29bcee8f6f703a5952b85fc2ffcbcfb0862db4 ba19dd366528b961430f5195c2e382420703074f git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 3b29bcee8f6f703a5952b85fc2ffcbcfb0862db4 1a48f94c63a078e7b6a2e59a637fc0858dc6510c git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 3b29bcee8f6f703a5952b85fc2ffcbcfb0862db4 9990cd4f8827bd1ae3fb6eb7407630d8d463c430 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 6.15  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.15 semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.18.19 6.18.* semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.19.9 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/9990cd4f8827bd1ae3fb6eb7407630d8d463c430">git.kernel.org/stable/c/9990cd4f8827bd1ae3fb6eb7407630d8d463c430</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/ba19dd366528b961430f5195c2e382420703074f">git.kernel.org/stable/c/ba19dd366528b961430f5195c2e382420703074f</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> |           |
| <a href="https://git.kernel.org/stable/c/1a48f94c63a078e7b6a2e59a637fc0858dc6510c">git.kernel.org/stable/c/1a48f94c63a078e7b6a2e59a637fc0858dc6510c</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](#) 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](#)