



# HID: asus: avoid memory leak in asus\_report\_fixup()

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

## Summary

<b>CVE</b>	CVE-2026-31524
<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 14:16:52 UTC
<b>Updated</b>	2026-04-22 14:16:52 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: HID: asus: avoid memory leak in asus\_report\_fixup() The

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 726765b43deb2b4723869d673cc5fc6f7a3b2059 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ede95cfcab8064d9a08813fbd7ed42cea8843dcf git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 2e4fe6b15c2f390c023b20d728b1a3fe7ea4f973 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 f20f17cffbe34fb330267e0f8084f5565f807444 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 7a6d6e4d8af044f94fa97e97af5ff2771e1fbedd git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 a41cc7c1668e44ff2c2d36f9a6353253ffc43e3c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 84724ac4821a160d47b84289adf139023027bdbb git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 2bad24c17742fc88973d6aea526ce1353f5334a3 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.253 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.203 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.168 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.131 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.80 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.21 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.11 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/2bad24c17742fc88973d6aea526ce1353f5334a3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	

<a href="https://git.kernel.org/stable/c/f20f17cffbe34fb330267e0f8084f5565f807444">git.kernel.org/stable/c/f20f17cffbe34fb330267e0f8084f5565f807444</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/2e4fe6b15c2f390c023b20d728b1a3fe7ea4f973">git.kernel.org/stable/c/2e4fe6b15c2f390c023b20d728b1a3fe7ea4f973</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/a41cc7c1668e44ff2c2d36f9a6353253ffc43e3c">git.kernel.org/stable/c/a41cc7c1668e44ff2c2d36f9a6353253ffc43e3c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/7a6d6e4d8af044f94fa97e97af5ff2771e1fbebdc">git.kernel.org/stable/c/7a6d6e4d8af044f94fa97e97af5ff2771e1fbebdc</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/ede95cfcab8064d9a08813fbd7ed42cea8843dcf">git.kernel.org/stable/c/ede95cfcab8064d9a08813fbd7ed42cea8843dcf</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/726765b43deb2b4723869d673cc5fc6f7a3b2059">git.kernel.org/stable/c/726765b43deb2b4723869d673cc5fc6f7a3b2059</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/84724ac4821a160d47b84289adf139023027bdbb">git.kernel.org/stable/c/84724ac4821a160d47b84289adf139023027bdbb</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>	canonic
NVD vulnerability detail	NVD	<a href="https://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](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](https://www.mitre.org/cve).

**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)