



HID: Add HID_CLAIMED_INPUT guards in raw_event callbacks missing them

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

Summary

CVE	CVE-2026-23382
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 11:16:38 UTC
Updated	2026-04-18 09:16:22 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: HID: Add HID_CLAIMED_INPUT guards in raw_event call

Risk And Classification

EPSS: 0.000320000 probability, percentile 0.090980000 (date 2026-04-18)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected d0742abaa1c396a26bb3d3ce2732988cd3faa020 b48284d7f0f76023b215a3409cdc989b5081eadf git
CNA	Linux	Linux	affected d0742abaa1c396a26bb3d3ce2732988cd3faa020 de316c1edf15bc30ff5e0d4c7b37c70fd41cf319 git
CNA	Linux	Linux	affected d0742abaa1c396a26bb3d3ce2732988cd3faa020 ac83b0d91a3f4f0c012ba9c85fb99436cddb1208 git
CNA	Linux	Linux	affected d0742abaa1c396a26bb3d3ce2732988cd3faa020 6e330889e6c8db99f04d4feb861d23de4e8fbb13 git
CNA	Linux	Linux	affected d0742abaa1c396a26bb3d3ce2732988cd3faa020 892dbaf46bb738dacf1fa663eadb3712c85868f0 git
CNA	Linux	Linux	affected d0742abaa1c396a26bb3d3ce2732988cd3faa020 20864e3e41c74cda253a9fa6b6fe093c1461a6a9 git
CNA	Linux	Linux	affected d0742abaa1c396a26bb3d3ce2732988cd3faa020 575122cd6569c4c4aa13c4c9958fea506724c788 gi
CNA	Linux	Linux	affected d0742abaa1c396a26bb3d3ce2732988cd3faa020 ecfa6f34492c493a9a1dc2900f3edeb01c79946b git
CNA	Linux	Linux	affected 2.6.35
CNA	Linux	Linux	unaffected 2.6.35 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 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.77 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.17 6.18.* semver

CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/ac83b0d91a3f4f0c012ba9c85fb99436cddb1208	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/892dbaf46bb738dacf1fa663eadb3712c85868f0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/6e330889e6c8db99f04d4feb861d23de4e8fbb13	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/575122cd6569c4c4aa13c4c9958fea506724c788	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b48284d7f0f76023b215a3409cdc989b5081eadf	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ecfa6f34492c493a9a1dc2900f3edeb01c79946b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/20864e3e41c74cda253a9fa6b6fe093c1461a6a9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/de316c1edf15bc30ff5e0d4c7b37c70fd41cf319	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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