



HID: asus: fix UAF via HID_CLAIMED_INPUT validation

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2025-39824
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-16 13:16:01 UTC
Updated	2026-05-12 13:17:13 UTC

Description In the Linux kernel, the following vulnerability has been resolved: HID: asus: fix UAF via HID_CLAIMED_INPUT validation A

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-416

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 9ce12d8be12c94334634dd57050444910415e45f 9a9e4a8317437bf944fa017c66e1e23a0
CNA	Linux	Linux	affected 9ce12d8be12c94334634dd57050444910415e45f 7170122e2ae4ab378c9cdf7cc54dea8b0
CNA	Linux	Linux	affected 9ce12d8be12c94334634dd57050444910415e45f eaae728e7335b5dbad70966e2bd520a7
CNA	Linux	Linux	affected 9ce12d8be12c94334634dd57050444910415e45f a8ca8fe7f516d27ece3afb995c3bd4d07c
CNA	Linux	Linux	affected 9ce12d8be12c94334634dd57050444910415e45f 5f3c0839b173f7f33415eb098331879e54
CNA	Linux	Linux	affected 9ce12d8be12c94334634dd57050444910415e45f c0d77e3441a92d0b4958193c9ac1c3f81
CNA	Linux	Linux	affected 9ce12d8be12c94334634dd57050444910415e45f 72a4ec018c9e9bc52f4f80eb3afb5d6a6t
CNA	Linux	Linux	affected 9ce12d8be12c94334634dd57050444910415e45f d3af6ca9a8c34bbd8cff32b469b84c9021
CNA	Linux	Linux	affected 4.10
CNA	Linux	Linux	unaffected 4.10 semver
CNA	Linux	Linux	unaffected 5.4.298 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.242 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.191 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.150 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.104 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.45 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.5 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
git.kernel.org/stable/c/9a9e4a8317437bf944fa017c66e1e23a0368b5c7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/c0d77e3441a92d0b4958193c9ac1c3f81c6f1d1c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/eaae728e7335b5dbad70966e2bd520a731fdf7b2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/7170122e2ae4ab378c9cdf7cc54dea8b0abbbca5	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/a8ca8fe7f516d27ece3afb995c3bd4d07dcbe62c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

git.kernel.org/stable/c/5f3c0839b173f7f33415eb098331879e547d1d2d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/72a4ec018c9e9bc52f4f80eb3afb5d6a6b752275	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d3af6ca9a8c34bbd8cff32b469b84c9021c9e7e4	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
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://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

CVE.report and Source URL Uptime Status status.cve.report