HID: amd_sfh: free driver_data after destroying hid device

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-46746
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-09-18 08:15:03 UTC
Updated	2026-04-23 13:54:03 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: HID: amd_sfh: free driver_data after destroying hid device

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	Debian	Debian Linux	11.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 4f567b9f8141a86c7d878fadf136e5d1408e3e61 86b4f5cf91ca03c08e3822ac89476a677a780bcc git
CNA	Linux	Linux	affected 4f567b9f8141a86c7d878fadf136e5d1408e3e61 775125c7fe38533aaa4b20769f5b5e62cc1170a0 git
CNA	Linux	Linux	affected 4f567b9f8141a86c7d878fadf136e5d1408e3e61 60dc4ee0428d70bcbb41436b6729d29f1cbdfb89 git
CNA	Linux	Linux	affected 4f567b9f8141a86c7d878fadf136e5d1408e3e61 adb3e3c1ddb5a23b8b7122ef1913f528d728937c git
CNA	Linux	Linux	affected 4f567b9f8141a86c7d878fadf136e5d1408e3e61 97155021ae17b86985121b33cf8098bcde00d497 git
CNA	Linux	Linux	affected 5.11
CNA	Linux	Linux	unaffected 5.11 semver
CNA	Linux	Linux	unaffected 5.15.167 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.110 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.51 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.10 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/97155021ae17b86985121b33cf8098bcde00d497	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/86b4f5cf91ca03c08e3822ac89476a677a780bcc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/60dc4ee0428d70bcbb41436b6729d29f1cbdfb89	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/775125c7fe38533aaa4b20769f5b5e62cc1170a0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Maili
git.kernel.org/stable/c/adb3e3c1ddb5a23b8b7122ef1913f528d728937c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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