



# HID: amd\_sfh: free driver\_data after destroying hid device

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

## Summary

<b>CVE</b>	CVE-2024-46746
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-09-18 08:15:03 UTC
<b>Updated</b>	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	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/86b4f5cf91ca03c08e3822ac89476a677a780bcc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/60dc4ee0428d70bcbb41436b6729d29f1cbdfb89	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/775125c7fe38533aaa4b20769f5b5e62cc1170a0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>	Maili
git.kernel.org/stable/c/ad3e3c1ddb5a23b8b7122ef1913f528d728937c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canc
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canc

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](#)