



# CVE-2025-29944

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

## Summary

<b>CVE</b>	CVE-2025-29944
<b>State</b>	PUBLISHED
<b>Assigner</b>	AMD
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-15 03:16:21 UTC
<b>Updated</b>	2026-05-15 03:16:21 UTC
<b>Description</b>	A buffer overflow vulnerability within AMD Sensor Fusion Hub Driver can allow a local attacker to write out of bounds, poter

## Risk And Classification

**Primary CVSS:** v4.0 6.8 MEDIUM from psirt@amd.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-120 | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
4.0	psirt@amd.com	Secondary	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	AMD	AMD Ryzen 4000 Series Mobile Processors With Radeon Graphics Formerly Codenamed Renoir	unaffected AMD
CNA	AMD	AMD Ryzen 7035 Series Processors With Radeon Graphics Formerly Codenamed Rembrandt R	unaffected AMD
CNA	AMD	AMD Athlon 3000 Series Mobile Processors With Radeon Graphics Formerly Codenamed Picasso	unaffected AMD
CNA	AMD	AMD Ryzen 7040 Series Mobile Processors With Radeon Graphics Formerly Codenamed Phoenix	unaffected AMD
CNA	AMD	AMD Ryzen 7020 Series Processors With Radeon Graphics Formerly Codenamed Mendocino	unaffected AMD
CNA	AMD	AMD Ryzen 7030 Series Mobile Processors With Radeon Graphics Formerly Codenamed Barcelo R	unaffected 7.04.
CNA	AMD	AMD Ryzen AI 300 Series Processors Formerly Codenamed Strix Point	unaffected AMD
CNA	AMD	AMD Ryzen 5000 Series Mobile Processors With Radeon Graphics Formerly Codenamed Cezanne	unaffected AMD
CNA	AMD	AMD Ryzen 5000 Series Mobile Processors With Radeon Graphics Formerly Codenamed Lucienne	unaffected AMD
CNA	AMD	AMD Ryzen 5000 Series Mobile Processors With Radeon Graphics Formerly Codenamed Barcelo	unaffected AMD
CNA	AMD	AMD Ryzen 8040 Series Mobile Processors With Radeon Graphics Formerly Codenamed Hawk Point	unaffected AMD
CNA	AMD	AMD Ryzen 3000 Series Mobile Processors With Radeon Graphics Formerly Codenamed Dali	unaffected AMD
CNA	AMD	AMD Ryzen 6000 Series Processors With Radeon Graphics Formerly Codenamed Rembrandt	unaffected AMD
CNA	AMD	AMD Ryzen AI Max 300 Series Processors	unaffected AMD
CNA	AMD	AMD Ryzen Embedded 8000 Series Processors	unaffected amd
CNA	AMD	AMD RYZEN Embedded 7000 Series Processors	unaffected amd

### References

Reference	Source	Link	Tags
www.amd.com/en/resources/product-security/bulletin/AMD-SB-4015.html	psirt@amd.com	www.amd.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Discovery Credit

**CNA:** Reported through AMD Bug Bounty Program (en)

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](#)