



CVE-2025-66664

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

Summary

CVE	CVE-2025-66664
State	PUBLISHED
Assigner	AMD
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 03:16:22 UTC
Updated	2026-05-15 03:16:22 UTC
Description	Insufficient parameter sanitization in AMD Secure Processor (ASP) TEE SOC Driver could allow an attacker to issue a mal

Risk And Classification

Primary CVSS: v4.0 4.6 MEDIUM from psirt@amd.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:L/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-125 | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	psirt@amd.com	Secondary	4.6	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:L/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	4.6	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

None

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:L/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 Radeon RX 6000 Series Graphics Products	unaffected AMD Software: Adrenalin Edition 25.12.1 (25.10.37.01)
CNA	AMD	AMD Radeon RX 7000 Series Graphics Products	unaffected AMD Software: Adrenalin Edition 25.11.1 (25.20.29.01)
CNA	AMD	AMD Radeon PRO W6000 Series Graphics Products	unaffected AMD Software: PRO Edition 25.Q4 (25.10.37.01)
CNA	AMD	AMD Radeon PRO W7000 Series Graphics Products	unaffected AMD Software: PRO Edition 25.Q3.1 (25.10.32)
CNA	AMD	AMD Instinct MI250	unaffected ROCm 7.0
CNA	AMD	AMD Instinct MI210	unaffected ROCm 7.0
CNA	AMD	AMD Instinct MI300X	unaffected ROCm 6.3.1
CNA	AMD	AMD Instinct MI325X	unaffected ROCm 6.3.1
CNA	AMD	AMD Instinct MI308X	unaffected ROCm 6.4.2
CNA	AMD	AMD Instinct MI300A	unaffected BKC 26 (ROCm 7.0.1)
CNA	AMD	AMD Radeon PRO V520	unaffected Contact your AMD Customer Engineering representati
CNA	AMD	AMD Radeon PRO V620	unaffected Contact your AMD Customer Engineering representati
CNA	AMD	AMD Radeon PRO V710	unaffected Contact your AMD Customer Engineering representati

References

Reference	Source	Link	Tags
www.amd.com/en/resources/product-security/bulletin/AMD-SB-6027.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

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](#)