CVE-2022-23826

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

Summary

CVE	CVE-2022-23826
State	PUBLISHED
Assigner	AMD
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 03:16:20 UTC
Updated	2026-05-15 03:16:20 UTC
Description	A TOCTOU (Time-Of-Check to Time-Of-Use) in the graphics interface may allow an attacker to load registers repeatedly cr

Risk And Classification

Primary CVSS: v4.0 1.8 LOW from psirt@amd.com

CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:N/VC:L/VI:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-367 | CWE-367 CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
4.0	psirt@amd.com	Secondary	1.8	LOW	CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	1.8	LOW	CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:N/VC:L/VI:L/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/MSC:X/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 3000 Series Mobile Processors With Radeon Graphics	unaffected PicassoPI-FP5 1.0.0.
CNA	AMD	AMD Athlon 3000 Series Mobile Processors With Radeon Graphics	unaffected PicassoPI-FP5 1.0.0.
CNA	AMD	AMD Athlon 3000 Series Desktop Processors With Radeon Graphics	unaffected ComboAM4v2 PI 1.2.
CNA	AMD	AMD Ryzen Embedded R1000 Series Processors	unaffected EmbeddedPI-FP5_1.
CNA	AMD	AMD Ryzen Embedded R2000 Series Processors	unaffected EmbeddedR2KPI-FP
CNA	AMD	AMD Ryzen Embedded V1000 Series Processors Formerly Codenamed Raven Ridge	unaffected EmbeddedPI-FP5_1.
CNA	AMD	AMD Ryzen Embedded V1000 Series Processors Formerly Codenamed Picasso	unaffected 120A
CNA	AMD	AMD Radeon RX 5000 Series Graphics Products	unaffected AMD Software: Adrer
CNA	AMD	AMD Radeon PRO W5000 Series Graphics Products	unaffected AMD Software: PRO
CNA	AMD	AMD Radeon RX 6000 Series Graphics Products	unaffected AMD Software: Adrer
CNA	AMD	AMD Radeon VII	unaffected AMD Software: Adrer
CNA	AMD	AMD Radeon RX Vega Series Graphics Cards	unaffected AMD Software: Adrer
CNA	AMD	AMD Radeon PRO W6000 Series Graphics Product	unaffected AMD Software: PRO
CNA	AMD	AMD Radeon PRO W6000 Series Graphics Products	unaffected AMD Software: PRO
CNA	AMD	AMD Radeon PRO WX 8000/9000 Series Graphics Cards	unaffected AMD Software: PRO
CNA	AMD	AMD Radeon PRO VII	unaffected AMD Software: PRO
CNA	AMD	AMD Instinct MI250	unaffected ROCm 6.4.2
CNA	AMD	AMD Instinct MI210	unaffected ROCm 6.4.2
CNA	AMD	AMD Radeon Instinct MI25	unaffected Contact your AMD Cu
CNA	AMD	AMD Radeon PRO V520	unaffected Contact your AMD Cu
CNA	AMD	AMD Radeon PRO V620	unaffected Contact your AMD Cu

References

Reference	Source	Link	Tags
www.amd.com/en/resources/product-security/bulletin/AMD-SB-6027.html	psirt@amd.com	www.amd.com	
www.amd.com/en/resources/product-security/bulletin/AMD-SB-4017.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.