CVE-2023-31316

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

Summary

CVE	CVE-2023-31316
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	Improperly preserved integrity of hardware configuration state during a power save/restore operation in the AMD Secure Pr

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from psirt@amd.com

CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/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-1304 | CWE-1304 CWE-1304 Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation

Version	Source	Type	Score	Severity	Vector
4.0	psirt@amd.com	Secondary	7.1	HIGH	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/E:X/C...
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

Low

Sub Conf.

Low

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/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 5000 Series Mobile Processors With Radeon Graphics	unaffected Cezanne-FP6 1.0.1.0
CNA	AMD	AMD Ryzen 7000 Series Desktop Processors	unaffected ComboAM5PI 1.0.0.a
CNA	AMD	AMD Ryzen 4000 Series Desktop Processors	unaffected ComboAM4v2 1.2.0.Ca
CNA	AMD	AMD Ryzen 5000 Series Desktop Processors With Radeon Graphics	unaffected ComboAM4v2 1.2.0.Ca
CNA	AMD	AMD Ryzen 7040 Series Mobile Processors With Radeon Graphics	unaffected PhoenixPI-FP8-FP7_1.1.0.0
CNA	AMD	AMD Ryzen 4000 Series Mobile Processors With Radeon Graphics	unaffected Renoir-FP6 1.0.0.D
CNA	AMD	AMD Ryzen 6000 Series Processors With Radeon Graphics	unaffected Rembrandt-FP7 1.0.0.A
CNA	AMD	AMD Ryzen 7020 Series Processors With Radeon Graphics	unaffected MendocinoPI-FT6_1.0.0.6
CNA	AMD	AMD Ryzen 7045 Series Mobile Processors With Radeon Graphics	unaffected DragonRangeFL1PI 1.0.0.3C
CNA	AMD	AMD Ryzen Embedded V2000 Series Processors	unaffected EmbeddedPI-FP6_1.0.0.9
CNA	AMD	AMD Ryzen Embedded V3000 Series Processors	unaffected Embedded-PI_FP7r2 1009
CNA	AMD	AMD Radeon RX 6000 Series Graphics Products	unaffected AMD Software: Adrenalin Edition 25.1
CNA	AMD	AMD Radeon RX 7000 Series Graphics Products	unaffected AMD Software: Adrenalin Edition 25.1
CNA	AMD	AMD Radeon PRO W7000 Series Graphics Products	unaffected AMD Software: PRO Edition 25.Q3.1 (
CNA	AMD	AMD Radeon PRO W6000 Series Graphics Products	unaffected AMD Software: PRO Edition 25.Q4 (25
CNA	AMD	AMD Instinct MI250	unaffected ROCm 6.4
CNA	AMD	AMD Instinct MI210	unaffected ROCm 6.4
CNA	AMD	AMD Radeon PRO V620	unaffected Contact your AMD Customer Engineer

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.

Free CVE JSON API cve.report/api

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