CVE-2023-31309

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

Summary

CVE	CVE-2023-31309
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	Improper validation in Power Management Firmware (PMFW) may allow an attacker with privileges to pass malformed work

Risk And Classification

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

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

Problem Types: CWE-129 | CWE-129 CWE-129 Improper Validation of Array Index

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:H/UI:N/VC:H/VI:N/VA:L/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/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

High

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:H/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/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 Radeon RX 6000 Series Graphics Products	unaffected AMD Software: Adrenalin Edition 23.12.1 (23.30.13.01
CNA	AMD	AMD Radeon PRO W6000 Series Graphics Products	unaffected AMD Software: PRO Edition 23.Q4
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

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.