CVE-2024-21962

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

Summary

CVE	CVE-2024-21962
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 Input Validation in the AMD RAID driver could allow an attacker to point to an arbitrary memory location potentially

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from psirt@amd.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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-1220 | CWE-1220 CWE-1220 Insufficient Granularity of Access Control

Version	Source	Type	Score	Severity	Vector
4.0	psirt@amd.com	Secondary	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/C...
4.0	CNA	CVSS	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/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 EPYC 4005 Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD EPYC 4004 Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen Threadripper PRO 3000 WX-Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen 5000 Series Mobile Processors With Radeon Graphics	unaffected No fix planned
CNA	AMD	AMD Ryzen Threadripper 7000 WX-Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen 9000HX Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen Threadripper PRO 5000 WX-Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen 3000 Series Desktop Processors	unaffected No fix planned
CNA	AMD	AMD Ryzen 3000 Series Mobile Processors With Radeon Graphics	unaffected No fix planned
CNA	AMD	AMD Ryzen 5000 Series Desktop Processors With Radeon Graphics	unaffected No fix planned
CNA	AMD	AMD Ryzen 5000 Series Desktop Processors	unaffected No fix planned
CNA	AMD	AMD Ryzen 7040 Series Mobile Processors With Radeon Graphics	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen 8040 Series Mobile Processors With Radeon Graphics	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen Z2 Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Athlon 3000 Series Mobile Processors With Radeon Graphics	unaffected No fix planned
CNA	AMD	AMD Ryzen 4000 Series Mobile Processors With Radeon Graphics	unaffected No fix planned
CNA	AMD	AMD Ryzen 6000 Series Processors With Radeon Graphics	unaffected No fix planned
CNA	AMD	AMD Ryzen AI 300 Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen 7020 Series Processors With Radeon Graphics	unaffected No fix planned
CNA	AMD	AMD Ryzen 7045 Series Mobile Processors With Radeon Graphics	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen AI Max 300 Series Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen Threadripper 9000 Series	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen 2000 Mobile Processors	unaffected No fix planned

CNA	AMD	AMD Ryzen 4000 Series Desktop Processors	unaffected No fix planned
CNA	AMD	AMD Ryzen 7000 Series Desktop Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen 8000 Series Desktop Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD Ryzen 9000 Series Desktop Processors	unaffected AMD RAID Software: 9.3.3.245
CNA	AMD	AMD EPYC Embedded 4005 Series Processors	unaffected Embedded EPYC_4005 Windows RAI

References

Reference	Source	Link	Tags
www.amd.com/en/resources/product-security/bulletin/AMD-SB-4016.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

Vendor Comments And Credit

Discovery Credit

CNA: Reported through AMD Bug Bounty Program (en)

There are currently no legacy QID mappings associated with this CVE.