



CVE-2026-0432

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

Summary

CVE	CVE-2026-0432
State	PUBLISHED
Assigner	AMD
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 02:16:23 UTC
Updated	2026-05-15 02:16:23 UTC
Description	Incorrect default permissions in the installation directory for the AMD chipset driver could allow an attacker to achieve privilege escalation.

Risk And Classification

Primary CVSS: v4.0 8.5 HIGH from psirt@amd.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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-276 | CWE-276 CWE-276 Incorrect Default Permissions

Version	Source	Type	Score	Severity	Vector
4.0	psirt@amd.com	Secondary	8.5	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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	8.5	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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 Ryzen 4000 Series Mobile Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 7035 Series Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Athlon 3000 Series Mobile Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 7040 Series Mobile Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 7020 Series Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 7045 Series Mobile Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 7000 Series Desktop Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 3000 Series Desktop Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen Threadripper PRO 3000 WX-Series Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 7030 Series Mobile Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen Threadripper PRO 3000 WX-Series Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen Threadripper 3000 Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 9000HX Series Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen AI 300 Series Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Athlon 3000 Series Desktop Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen Threadripper PRO 5000 WX-Series Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen Threadripper 7000 Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen Threadripper PRO 7000 WX-Series Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen Threadripper PRO 7000 WX-Series Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 8000 Series Desktop Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 9000 Series Desktop Processors	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 5000 Series Mobile Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets
CNA	AMD	AMD Ryzen 5000 Series Mobile Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipsets

CNA	AMD	AMD Ryzen 4000 Series Desktop Processors	unaffected AMD Ryzen™ Chipset
CNA	AMD	AMD Ryzen 5000 Series Desktop Processors	unaffected AMD Ryzen™ Chipset
CNA	AMD	AMD Ryzen 5000 Series Desktop Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipset
CNA	AMD	AMD Ryzen 3000 Series Desktop Processors	unaffected AMD Ryzen™ Chipset
CNA	AMD	AMD Ryzen 8040 Series Mobile Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipset
CNA	AMD	AMD Ryzen 6000 Series Processors With Radeon Graphics	unaffected AMD Ryzen™ Chipset
CNA	AMD	AMD Ryzen AI Max 300 Series Processors	unaffected AMD Ryzen™ Chipset
CNA	AMD	AMD Ryzen AI 400 Series Processors	unaffected AMD Ryzen™ Chipset
CNA	AMD	AMD Ryzen Embedded R1000 Series Processors	unaffected Q1 - 2026 AMD Embedded
CNA	AMD	AMD Ryzen Embedded R2000 Series Processors	unaffected Q1 - 2026 AMD Embedded
CNA	AMD	AMD Ryzen Embedded V1000 Series Processors Formerly Codenamed Raven Ridge	unaffected Q1 - 2026 AMD Embedded
CNA	AMD	AMD Ryzen Embedded V2000 Series Processors	unaffected Q1 - 2026 AMD Embedded
CNA	AMD	AMD EPYC Embedded 8004 Series Processors	unaffected Q2-2026 AMD Embedded
CNA	AMD	AMD Ryzen Embedded 8000 Series Processors	unaffected Q1- 2026 AMD Embedded
CNA	AMD	AMD Ryzen Embedded 7000 Series Processors	unaffected Q1- 2026 AMD Embedded
CNA	AMD	AMD EPYC Embedded 9005 Series Processors	unaffected Q2-2026 AMD Embedded
CNA	AMD	AMD Ryzen Embedded 9000 Series Processors	unaffected Q1- 2026 AMD Embedded
CNA	AMD	AMD EPYC 9004 Series Processors	unaffected AMD Server Software
CNA	AMD	AMD EPYC 7003 Series Processors	unaffected AMD Server Software
CNA	AMD	AMD EPYC 7002 Series Processors	unaffected AMD Server Software
CNA	AMD	AMD EPYC 7001 Series Processors	unaffected AMD Server Software
CNA	AMD	AMD EPYC 4004 Series Processors	unaffected AMD Chipset Driver & BIOS
CNA	AMD	AMD EPYC 9005 Series Processors	unaffected AMD Server Software
CNA	AMD	AMD Instinct MI300A Series Processors	unaffected AMD Server Software
CNA	AMD	AMD EPYC 9V64H Processor	unaffected AMD Server Software
CNA	AMD	AMD EPYC 8004 Series Processors	unaffected AMD Server Software
CNA	AMD	AMD EPYC 4005 Series Processors	unaffected AMD Chipset Driver & BIOS

References

Reference	Source	Link	Tags
www.amd.com/en/resources/product-security/bulletin/AMD-SB-3047.html	psirt@amd.com	www.amd.com	
www.amd.com/en/resources/product-security/bulletin/AMD-SB-4015.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.

© [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](#)