CVE-2025-54502

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

Summary

CVE	CVE-2025-54502
State	PUBLISHED
Assigner	AMD
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-16 20:16:37 UTC
Updated	2026-04-16 20:16:37 UTC
Description	Incorrect use of boot service in the AMD Platform Configuration Blob (APCB) SMM driver could allow a privileged attacker v

Risk And Classification

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

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

Problem Types: CWE-668 | CWE-668 CWE-668 Exposure of Resource to Wrong Sphere

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

High

Integrity

High

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:H/AT:N/PR:H/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/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 9004 Series Processors	unaffected GenoaPI_1.0.0.H
CNA	AMD	AMD EPYC 7003 Series Processors	unaffected MilanPI-SP3_1.0.0.J
CNA	AMD	AMD EPYC 7002 Series Processors	unaffected Rome-1.0.0.P
CNA	AMD	AMD EPYC 4004 Series Processors	unaffected ComboAM5PI 1.0.0.c
CNA	AMD	AMD EPYC 9005 Series Processors	unaffected TurinPI-SP5_1.0.0.9
CNA	AMD	AMD Instinct MI300A Series Processors	unaffected MI300A 1.0.0.C
CNA	AMD	AMD EPYC 9V64H Processor	unaffected MI300C 1.0.0.3
CNA	AMD	AMD EPYC 8004 Series Processors	unaffected GenoaPI_1.0.0.H
CNA	AMD	AMD Ryzen 4000 Series Mobile Processors With Radeon Graphics	unaffected RenoirPI-FP6 1.0.0.E
CNA	AMD	AMD Ryzen 7035 Series Processors With Radeon Graphics	unaffected RembrandtPI-FP7_1.
CNA	AMD	AMD Athlon 3000 Series Mobile Processors With Radeon Graphics	unaffected PicassoPI-FP5_1.0.1
CNA	AMD	AMD Ryzen 7040 Series Mobile Processors With Radeon Graphics	unaffected PhoenixPI-FP8-FP7_
CNA	AMD	AMD Ryzen 7020 Series Processors With Radeon Graphics	unaffected MendocinoPI-FT6_1.
CNA	AMD	AMD Ryzen 7045 Series Mobile Processors With Radeon Graphics	unaffected DragonRangeFL1PI
CNA	AMD	AMD Ryzen 7000 Series Desktop Processors	unaffected ComboAM5PI 1.0.0.c
CNA	AMD	AMD Ryzen 3000 Series Desktop Processors	unaffected ComboAM4v2PI 1.2.(
CNA	AMD	AMD Ryzen Threadripper PRO 3000 WX-Series Processors	unaffected ChagallWSPI-sWRX8
CNA	AMD	AMD Ryzen 7030 Series Mobile Processors With Radeon Graphics	unaffected CezannePI-FP6_1.0.
CNA	AMD	AMD Ryzen Threadripper PRO 3000 WX-Series Processors	unaffected CastlePeakWSPI-sW
CNA	AMD	AMD Ryzen 9000HX Series Processors	unaffected FireRangeFL1PI 1.0.(
CNA	AMD	AMD Ryzen AI 300 Series Processors	unaffected StrixKrackanPI-FP8_
CNA	AMD	AMD Ryzen Threadripper PRO 5000 WX-Series Processors	unaffected ChagallWSPI-sWRX8
CNA	AMD	AMD Ryzen Threadripper PRO 7000 WX-Series Processors	unaffected StormPeakPI-SP6 1.(

CNA	AMD	AMD Ryzen Threadripper PRO 7000 WX-Series Processors	unaffected StormPeakPI-SP6_1.
CNA	AMD	AMD Ryzen 7000 Series Desktop Processors	unaffected ComboAM5PI 1.1.0.3
CNA	AMD	AMD Ryzen 7000 Series Desktop Processors	unaffected ComboAM5PI 1.2.0.3
CNA	AMD	AMD Ryzen 8000 Series Desktop Processors	unaffected ComboAM5PI 1.1.0.3
CNA	AMD	AMD Ryzen 8000 Series Desktop Processors	unaffected ComboAM5PI 1.2.0.3
CNA	AMD	AMD Ryzen 9000 Series Desktop Processors	unaffected ComboAM5PI 1.2.0.3
CNA	AMD	AMD Ryzen 5000 Series Mobile Processors With Radeon Graphics	unaffected CezannePI-FP6_1.0.
CNA	AMD	AMD Ryzen 5000 Series Mobile Processors With Radeon Graphics	unaffected CezannePI-FP6_1.0.
CNA	AMD	AMD Ryzen 4000 Series Desktop Processors	unaffected ComboAM4v2PI 1.2.(
CNA	AMD	AMD Ryzen 5000 Series Desktop Processors	unaffected ComboAM4v2PI 1.2.(
CNA	AMD	AMD Ryzen 5000 Series Desktop Processors With Radeon Graphics	unaffected ComboAM4v2PI 1.2.(
CNA	AMD	AMD Ryzen 3000 Series Desktop Processors	unaffected ComboAM4PI 1.0.0.1
CNA	AMD	AMD Ryzen 8040 Series Mobile Processors With Radeon Graphics	unaffected PhoenixPI-FP8-FP7_
CNA	AMD	AMD Ryzen 3000 Series Mobile Processors With Radeon Graphics	unaffected PicassoPI-FP5_1.0.1
CNA	AMD	AMD Ryzen 6000 Series Processors With Radeon Graphics	unaffected RembrandtPI-FP7_1.
CNA	AMD	AMD Ryzen AI Max 300 Series Processors	unaffected StrixHaloPI-FP11_1.(
CNA	AMD	AMD Ryzen Z1 Series Processors	unaffected StrixKrackanPI-FP8_
CNA	AMD	AMD Ryzen Z1 Series Processors	unaffected PhoenixPI-FP8-FP7_
CNA	AMD	AMD Ryzen Z2 Series Processors Extreme	unaffected StrixKrackanPI-FP8_
CNA	AMD	AMD Ryzen Z2 Series Processors	unaffected PhoenixPI-FP8-FP7_
CNA	AMD	AMD Ryzen Z2 Series Processors Go	unaffected RembrandtPI-FP7_1.
CNA	AMD	AMD Ryzen Threadripper PRO 7000 WX-Series Processors	unaffected ShimadaPeakPI-SP6
CNA	AMD	AMD Ryzen Threadripper 7000 Processors	unaffected ShimadaPeakPI-SP6
CNA	AMD	AMD Ryzen Threadripper 9000 Processors	unaffected ShimadaPeakPI-SP6
CNA	AMD	AMD Ryzen Threadripper PRO 9000 WX-Series Processors	unaffected ShimadaPeakPI-SP6
CNA	AMD	AMD Ryzen AI 300 Series Processors	unaffected StrixKrackanPI-FP8_
CNA	AMD	AMD Ryzen 7000 Series Desktop Processors Formerly Codenamed Raphael	unaffected ComboAM5PI 1.2.8.(
CNA	AMD	AMD Ryzen 8000 Series Desktop Processors Formerly Codenamed Phoenix	unaffected ComboAM5PI 1.2.8.(
CNA	AMD	AMD Ryzen 9000 Series Desktop Processors Formerly Codenamed Granite Ridge	unaffected ComboAM5PI 1.2.8.(
CNA	AMD	AMD EPYC Embedded 7003 Series Processors	unaffected EmbMilanPI-SP3 1.0
CNA	AMD	AMD EPYC Embedded 9004 Series Processors Formerly Codenamed Genoa	unaffected EmbGenoaPI-SP5 1.
CNA	AMD	AMD EPYC Embedded 7002 Series Processors	unaffected EmbRomePI-SP3 1.(
CNA	AMD	AMD Ryzen Embedded R1000 Series Processors	unaffected EmbeddedPI-FP5 12
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 12
CNA	AMD	AMD Ryzen Embedded 5000 Series Processors	unaffected EmbAM4PI 1.0.0.9

CNA	AMD	AMD Ryzen Embedded V2000 Series Processors	unaffected EmbeddedPI-FP6_1.
CNA	AMD	AMD Ryzen Embedded V3000 Series Processors	unaffected Embedded-PI_FP7r2
CNA	AMD	AMD EPYC Embedded 9004 Series Processors Formerly Codenamed Bergamo	unaffected EmbGenoaPI-SP5 1.
CNA	AMD	AMD EPYC Embedded 8004 Series Processors	unaffected EmbGenoaPI-SP5 1.
CNA	AMD	AMD Ryzen Embedded 9000 Series Processors	unaffected EmbeddedAM5PI 1.0
CNA	AMD	AMD Ryzen Embedded 8000 Series Processors	unaffected EmbeddedPhoenixPI
CNA	AMD	AMD Ryzen Embedded 7000 Series Processors	unaffected EmbeddedAM5PI 1.0
CNA	AMD	AMD EPYC Embedded 9005 Series Processors	unaffected EmbeddedTurinPI_S

References

Reference	Source	Link	Tags
www.amd.com/en/resources/product-security/bulletin/AMD-SB-7054.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.

© 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 registred 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**