# CVE-2026-0438

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-0438 |
| **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** | A System Management Mode (SMM) handler could perform a callout to code located in non-SMM/untrusted memory. A hig |

## Risk And Classification

**Primary CVSS:** v4.0 5.4 MEDIUM from psirt@amd.com

CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:A/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-1072 | CWE-1072 CWE-1072 Call to Function Pointer from Untrusted Control Sphere in SMM

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | psirt@amd.com | Secondary | 5.4 | MEDIUM | CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/C... |
| 4.0 | CNA | CVSS | 5.4 | MEDIUM | CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N |

## CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

Active

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:A/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 Ryzen 7040 Series Mobile Processors With Radeon Graphics | unaffected PhoenixPI-FP8-FP7_1.2 |
| CNA | AMD | AMD Ryzen 7045 Series Mobile Processors With Radeon Graphics | unaffected DragonRangeFL1PI 1.0. |
| CNA | AMD | AMD Ryzen 7000 Series Desktop Processors | unaffected ComboAM5PI 1.0.0.d |
| CNA | AMD | AMD Ryzen 9000HX Series Processors | unaffected FireRangeFL1PI 1.0.0.0 |
| CNA | AMD | AMD Ryzen AI 300 Series Processors | unaffected StrixKrackanPI-FP8_1.1 |
| CNA | AMD | AMD Ryzen Threadripper PRO 7000 WX-Series Processors | unaffected StormPeakPI-SP6 1.0.0. |
| CNA | AMD | AMD Ryzen Threadripper PRO 7000 WX-Series Processors | unaffected StormPeakPI-SP6_1.1.0 |
| CNA | AMD | AMD Ryzen 7000 Series Desktop Processors | unaffected ComboAM5PI 1.1.0.3f |
| CNA | AMD | AMD Ryzen 7000 Series Desktop Processors | unaffected ComboAM5PI_1.2.0.3i |
| CNA | AMD | AMD Ryzen 8000 Series Desktop Processors | unaffected ComboAM5PI 1.1.0.3f |
| CNA | AMD | AMD Ryzen 8000 Series Desktop Processors | unaffected ComboAM5PI_1.2.0.3i |
| CNA | AMD | AMD Ryzen 9000 Series Desktop Processors | unaffected ComboAM5PI_1.2.0.3i |
| CNA | AMD | AMD Ryzen 8040 Series Mobile Processors With Radeon Graphics | unaffected PhoenixPI-FP8-FP7_1.2 |
| CNA | AMD | AMD Ryzen AI Max 300 Series Processors | unaffected StrixHaloPI-FP11_1.0.0. |
| CNA | AMD | AMD Ryzen Z1 Series Processors | unaffected PhoenixPI-FP8-FP7_1.2 |
| CNA | AMD | AMD Ryzen Z1 Series Processors | unaffected PhoenixPI-FP8-FP7_1.2 |
| CNA | AMD | AMD Ryzen Z2 Series Processors Extreme | unaffected StrixKrackanPI-FP8_1.1 |
| CNA | AMD | AMD Ryzen Z2 Series Processors | unaffected PhoenixPI-FP8-FP7_1.2 |
| CNA | AMD | AMD Ryzen Threadripper PRO 7000 WX-Series Processors | unaffected ShimadaPeakPI-SP6 1.0 |
| CNA | AMD | AMD Ryzen Threadripper 7000 Processors | unaffected ShimadaPeakPI-SP6 1.0 |
| CNA | AMD | Not Public | unaffected StrixKrackanPI-FP8_1.1 |
| CNA | AMD | AMD Ryzen Threadripper 9000 Processors | unaffected ShimadaPeakPI-SP6 1.0 |

| | | | |
|---|---|---|---|
| CNA | AMD | AMD Ryzen Threadripper PRO 9000 WX-Series Processors | unaffected ShimadaPeakPI-SP6 1.( |
| CNA | AMD | AMD Ryzen 7000 Series Desktop Processors Formerly Codenamed Raphael | unaffected ComboAM5PI_1.3.0.0 |
| CNA | AMD | AMD Ryzen 8000 Series Desktop Processors Formerly Codenamed Phoenix | unaffected ComboAM5PI_1.3.0.0 |
| CNA | AMD | AMD Ryzen 9000 Series Desktop Processors Formerly Codenamed Granite Ridge | unaffected ComboAM5PI_1.3.0.0 |
| CNA | AMD | AMD Ryzen Embedded 9000 Series Processors | unaffected EmbeddedAM5PI 1.0.0.5 |
| CNA | AMD | AMD Ryzen Embedded 8000 Series Processors | unaffected EmbeddedPhoenixPI-FP |
| CNA | AMD | AMD Ryzen Embedded 7000 Series Processors | unaffected EmbeddedAM5PI 1.0.0.5 |
| CNA | AMD | AMD EPYC 4004 Series Processors | unaffected ComboAM5PI 1.0.0.d / C |
| CNA | AMD | AMD EPYC 4005 Series Processors | unaffected ComboAM5PI_1.2.0.3i |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| www.amd.com/en/resources/product-security/bulletin/AMD-SB-3030.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.