Security Advisory 2024-075

Vulnerabilities in AMD CPUs

August 12, 2024 — v1.0

TLP:CLEAR

History:

- *12/08/2024 — v1.0 – Initial publication*

Summary

On August 9, 2024, AMD disclosed a high-severity vulnerability, **CVE-2023-31315** (SinkClose), affecting multiple generations of EPYC, Ryzen, and Threadripper processors. The flaw allows attackers with kernel-level access to gain Ring-2 privileges, potentially installing undetectable malware by modifying System Management Mode (SMM) settings [1].

Technical Details

The SinkClose vulnerability (CVSS score: 7.5) enables privilege escalation to Ring-2, allowing attackers to modify SMM settings even with SMM Lock enabled. This can disable security features and facilitate persistent, nearly undetectable malware.

Affected Products

According to AMD's advisory, the following models are affected [1]:

- EPYC 1st, 2nd, 3rd, and 4th generations
- EPYC Embedded 3000, 7002, 7003, and 9003, R1000, R2000, 5000, and 7000
- Ryzen Embedded V1000, V2000, and V3000
- Ryzen 3000, 5000, 4000, 7000, and 8000 series
- Ryzen 3000 Mobile, 5000 Mobile, 4000 Mobile, and 7000 Mobile series
- Ryzen Threadripper 3000 and 7000 series
- AMD Threadripper PRO (Castle Peak WS SP3, Chagall WS)
- AMD Athlon 3000 series Mobile (Dali, Pollock)
- AMD Instinct MI300A

Recommendations

CERT-EU recommends applying AMD's available mitigations immediately [2].

References

[1] https://www.bleepingcomputer.com/news/security/new-amd-sinkclose-flaw-helps-install-nearly-undetectable-malware/

[2] https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7014.html