مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - AMD

Tracking #:432316880

Date:18-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that AMD has released security updates to address multiple vulnerabilities in its EPYC and Ryzen Embedded processors. These vulnerabilities could allow arbitrary code execution, memory corruption, or privilege escalation.

TECHNICAL DETAILS:

Notable Vulnerabilities:

- **CVE-2023-31342, CVE-2023-31343, CVE-2023-31345** (CVSS 7.5, High): Stem from improper input validation in the SMM handler, potentially allowing a privileged attacker to overwrite SMRAM and execute arbitrary code.
- **CVE-2023-31352** (CVSS 6.0, Medium): Affects SEV firmware, allowing an attacker with privileges to read unencrypted memory, potentially leading to loss of guest private data.
- **CVE-2023-20515** (CVSS 5.7, Medium): Improper access control in the fTPM driver could allow a privileged attacker to corrupt system memory, compromising data integrity.
- **CVE-2023-20582** (CVSS 5.3, Medium): Flaws in the IOMMU could let attackers bypass RMP checks in SEV-SNP, impacting guest memory security.
- **CVE-2023-31356** (CVSS 4.4, Medium): Incomplete system memory cleanup in SEV firmware could corrupt guest private memory, affecting data integrity.

Affected Products: These vulnerabilities impact the following AMD processors:

- **EPYC Embedded Series:** 3000, 7002, 7003, 9004
- **Ryzen Embedded Series:** R1000, R2000, 5000, 7000, V1000, V2000, V3000

Firmware Updates: To address these vulnerabilities, AMD has released key firmware updates, including:

- **EmbMilanPI-SP3 1.0.0.8** (2024-01-15) for EPYC Embedded 7003
- **EmbGenoaPI-SP5 1.0.0.7** (2024-07-15) for EPYC Embedded 9004
- **EmbeddedPI-FP5 1.2.0.C** (2024-06-14) for Ryzen Embedded R1000
- **EmbeddedAM5PI 1.0.0.1** (2024-07-31) for Ryzen Embedded 7000

RECOMMENDATIONS:

1. **Apply Firmware Updates Immediately**: Prioritize patching affected systems using AMD's provided PI firmware versions.
2. **OEMs**: Ensure that BIOS and firmware patches are properly deployed.
3. **Enforce Access Controls**: Restrict privileges to prevent unauthorized firmware modifications.
4. **Monitor Systems**: Audit for unusual activity indicating exploitation attempts.
5. **Secure Configurations**: Disable unnecessary services and enforce least-privilege principles.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.amd.com/en/resources/product-security/bulletin/amd-sb-5004.html