مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in AMD processors

Tracking #:432316835

Date:06-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in AMD processors that could potentially be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2024-56161**
- CVSS score 7.2 High
- A high-severity vulnerability that could allow attackers to load malicious CPU microcode on unpatched devices.
- The vulnerability stems from an improper signature verification weakness in AMD's CPU ROM microcode patch loader. Attackers with local administrator privileges can exploit this flaw, potentially compromising the confidentiality and integrity of guests running under AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP).
- Successful exploitation could lead to:
    - Loss of confidentiality and integrity for confidential guests running under AMD SEV-SNP
    - Compromise of confidential computing workloads protected by SEV-SNP
    - Potential compromise of Dynamic Root of Trust Measurement

Affected Products:

The vulnerability impacts multiple AMD EPYC processor families, including:

- Naples (EPYC 7001 Series)
- Rome (EPYC 7002 Series)
- Milan and Milan-X (EPYC 7003 Series)
- Genoa and Genoa-X (EPYC 9004 Series)
- Bergamo and Siena (EPYC 9004 Series)

Mitigation:

- AMD has released microcode updates for all affected platforms.
- Some platforms require an additional SEV firmware update for SEV-SNP attestation.
- Users need to update their system BIOS and reboot to enable the mitigation

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by AMD.

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://nvd.nist.gov/vuln/detail/CVE-2024-56161