مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

High Severity Vulnerability in MSI Motherboards

Tracking #:432316154

Date:16-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed MSI has disclosed a significant vulnerability, tracked as CVE-2024-36877, affecting a variety of its motherboards.

TECHNICAL DETAILS:

MSI has disclosed a significant vulnerability, tracked as **CVE-2024-36877,** affecting a variety of its motherboards. This vulnerability, located in the System Management Mode (SMM) handler, poses a risk of arbitrary code execution, which could lead to complete system compromise. The SMM is a privileged environment in modern computer firmware responsible for critical functions like power management and system updates, making it a prime target for attackers.

- **CVE-2024-36877** | CVSS Score: 8.2- SMM Handler Vulnerability
- **Affected Versions**: Intel 300 or later and AM4, AM5 chipset.
- **Public Exploit Code**: Available, the availability of proof-of-concept exploit code increases the likelihood of attacks, emphasizing the urgency of patching.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the latest BIOS version for respective motherboard as soon as possible.

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://csr.msi.com/global/product-security-advisories