



مجلس الأمن السيبراني

CYBER SECURITY COUNCIL



High-Impact UEFI Vulnerability in Phoenix Firmware

Tracking #:432315973

Date:24-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability has been identified in Phoenix SecureCore UEFI firmware, impacting hundreds of PC models from major manufacturers like Lenovo, Acer, Dell, and HP.

TECHNICAL DETAILS:

A high-impact vulnerability (**CVE-2024-0762**) has been identified in Phoenix SecureCore UEFI firmware, impacting hundreds of PC models from major manufacturers like Lenovo, Acer, Dell, and HP. This vulnerability allows attackers to potentially gain persistent control over the infected device.

Key Points:

Affected Systems: PCs with Intel processors and Phoenix SecureCore UEFI firmware

Exploit: Buffer overflow in UEFI code handling Trusted Platform Module (TPM) configuration

Impact: Potential for attackers to gain persistence and execute arbitrary code at the UEFI level, bypassing traditional security measures.

Severity: High (CVSS score: 7.5)

Patch Status: Patch available from Phoenix Technologies (distributed in April 2024)

Recommendation: Update your UEFI firmware as soon as possible. Refer to device manufacturer for specific instructions.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to check with device manufacturer for UEFI firmware updates and apply the update 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://www.phoenix.com/security-notifications/cve-2024-0762/>