

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Phoenix UEFI Firmware Flaw Exposes Multiple Intel CPUs to Risk

Date of Publication

June 24, 2024

Admiralty Code

A1

TA Number

TA2024241




# Summary

**First Seen:** May 14, 2024

**Affected Product:** Phoenix SecureCore UEFI firmware

**Impact:** The CVE-2024-0762 vulnerability in Phoenix SecureCore UEFI firmware affects many Intel Core processors, allowing local attackers to execute code within the UEFI firmware and escalate privileges. This can lead to severe system compromise, including persistent control that bypasses typical security measures. Lenovo has released BIOS updates to address the issue, and users should promptly apply these patches to protect their systems.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-0762	UEFICanHazBufferOverflow (Phoenix SecureCore UEFI firmware Buffer Overflow Vulnerability)	Phoenix SecureCore UEFI firmware			

# Vulnerability Details

## #1

A recent vulnerability identified in the Phoenix SecureCore UEFI firmware has been found to affect a wide range of PCs and servers using various Intel Core processors. This vulnerability, designated CVE-2024-0762, and dubbed 'UEFICANHAZBUFFEROVERFLOW', lies in the Trusted Platform Module (TPM) configuration and allows local attackers to escalate privileges and execute arbitrary code within the UEFI firmware. Such a flaw can have severe consequences, including the potential to compromise the entire system before the operating system even loads, thus bypassing traditional security measures.

## #2

The impact of this vulnerability is particularly concerning due to its potential for extensive exploitation. Attackers with local access could leverage this flaw to gain persistent control over affected systems, making it extremely difficult to detect and remove malicious code. The ability to execute code at the firmware level means that attackers can manipulate system settings, disable security features, and install persistent malware that survives reboots and system reinstalls. This level of control poses a significant threat to both individual users and enterprise environments, potentially leading to data breaches, system failures, and more.

# #3

Given the severe implications of this vulnerability, it is crucial for affected users and organizations to respond swiftly. Lenovo has already released BIOS updates to address the issue, and it is expected that other manufacturers will follow suit. Users should ensure their devices are up-to-date with the latest firmware patches. For those managing multiple devices, implementing a strategy for regular vulnerability scanning and prompt patching is essential to maintain system security and integrity.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-0762	Phoenix SecureCore for Intel Kaby Lake: from 4.0.1.1 before 4.0.1.998; Phoenix SecureCore for Intel Coffee Lake: from 4.1.0.1 before 4.1.0.562; Phoenix SecureCore for Intel Ice Lake: from 4.2.0.1 before 4.2.0.323; Phoenix SecureCore for Intel Comet Lake: from 4.2.1.1 before 4.2.1.287; Phoenix SecureCore for Intel Tiger Lake: from 4.3.0.1 before 4.3.0.236; Phoenix SecureCore for Intel Jasper Lake: from 4.3.1.1 before 4.3.1.184; Phoenix SecureCore for Intel Alder Lake: from 4.4.0.1 before 4.4.0.269; Phoenix SecureCore for Intel Raptor Lake: from 4.5.0.1 before 4.5.0.218; Phoenix SecureCore for Intel Meteor Lake: from 4.5.1.1 before 4.5.1.15	cpe:2.3:a:phoenix:secure_for_intel_kaby_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_coffee_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_ice_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_comet_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_tiger_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_jasper_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_alder_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_raptor_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_alder_lake:*:*:*:*:*:* cpe:2.3:a:phoenix:secure_for_intel_meteor_lake:*:*:*:*:*:*	CWE-120

# Recommendations



**Apply Firmware Updates:** Ensure that you install the latest BIOS updates from your device manufacturer. Lenovo and other affected manufacturers have released updates to address this vulnerability.



**Regular Scanning:** Implement a strategy for regular scanning of devices for firmware vulnerabilities. Use tools and services that can identify and assess potential security issues in your firmware.



**Access Control:** Limit physical access to systems, as the vulnerability requires local access to exploit. Implement strict access controls and monitor for unusual activity.



**Best Practices:** Follow general security best practices, such as keeping software and firmware up to date, using strong authentication mechanisms, and employing endpoint protection solutions.

## Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1499</u> Endpoint Denial of Service



## Patch Link

<https://www.phoenix.com/security-notifications/cve-2024-0762/>



## References

<https://eclipsium.com/blog/ueficanhazbufferoverflow-widespread-impact-from-vulnerability-in-popular-pc-and-server-firmware/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**June 24, 2024 • 1:30 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)