

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## **MSI Installer Flaw Enables Privilege Escalation on Windows Systems**

Date of Publication

July 4, 2024

Admiralty Code

A1

TA Number

TA2024256

# Summary

**First Seen:** July 2024

**Affected Products:** MSI Center

**Impact:** A critical local privilege escalation vulnerability has been discovered in MSI Center versions 2.0.36.0 and earlier, allowing low-privileged users to escalate their privileges on Windows systems. This security flaw, tracked as CVE-2024-37726, stems from insecure file operations performed by the MSI Center application running with NT AUTHORITY\SYSTEM privileges.

## 🔧 CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-37726	MSI Center Privilege Escalation Vulnerability	MSI Center	✗	✗	✓

# Vulnerability Details

## #1

A critical security flaw has been discovered in MSI Center versions below 2.0.36.0, running on Windows OS. This vulnerability allows a low-privileged user to overwrite or delete high-privileged and critical files, potentially causing significant system impact. MSI Center is a software suite developed by Micro-Star International (MSI), designed to optimize and enhance the performance of MSI hardware components and devices, primarily targeting gaming PCs and laptops.

## #2

The root of the issue lies in the MSI Center application, which operates with NT AUTHORITY\SYSTEM privileges. It writes files to directories that can be controlled by low-privileged users, opening the door to manipulation and exploitation. Specifically, a low-privileged user can create a directory and set an OpLock on a file. This enables the MSI Center application to overwrite or delete files with SYSTEM privileges.

## #3

An attacker could exploit this flaw by using the "Export System Info" function in MSI Center. By setting an OpLock on a file, moving the original file, and creating a junction to the target file, the attacker can cause the MSI Center to overwrite or delete critical files. This could also lead to the installation of programs without admin rights and the placement of malicious payloads in startup locations, which would be triggered when an administrator logs in.

## #4

Fortunately, MSI has addressed this vulnerability in version 2.0.38.0 of MSI Center. Users are strongly urged to update to this version to mitigate the associated risks. This incident highlights the importance of proper file system access controls and the dangers posed by applications with elevated privileges. To ensure your system's integrity and protection, it's crucial to prioritize updating MSI Center to the latest version.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-37726	MSI Center versions 2.0.36.0 and earlier	cpe:2.3:a:micro-star_international:msi_center:2.0.36.0:*:*:*:*:*	CWE-266

## Recommendations



**Update:** To mitigate the risk posed by CVE-2024-37726, MSI has released a patched version, 2.0.38.0, which addresses the vulnerability. Users are strongly advised to update to this version to reduce the risk of exploitation.



**Conduct Thorough Security Audits:** To safeguard against potential vulnerabilities and ensure the integrity of our systems, it is imperative to conduct regular and comprehensive security audits. These audits serve as proactive measures to identify and mitigate risks, ultimately fortifying our defenses against cyber threats.



**Least Privilege:** Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.



**Automated Updates:** Utilize automated tools and mechanisms to streamline the update process where feasible. Automated updates can reduce manual effort and ensure timely deployment of critical patches.

# Potential MITRE ATT&CK TTPs

<b>TA0042</b> Resource Development	<b>TA0002</b> Execution	<b>TA0004</b> Privilege Escalation	<b>TA0040</b> Impact
<b>T1588</b> Obtain Capabilities	<b>T1588.006</b> Vulnerabilities	<b>T1059</b> Command and Scripting Interpreter	<b>T1068</b> Exploitation for Privilege Escalation
<b>T1565</b> Data Manipulation	<b>T1203</b> Exploitation for Client Execution		

## Patch Details

To address the vulnerability (CVE-2024-37726), MSI has released a patched version, 2.0.38.0, which fixes the vulnerability. Users are urged to update to this version to mitigate risks.

Links: <https://www.msi.com/Landing/MSI-Center>

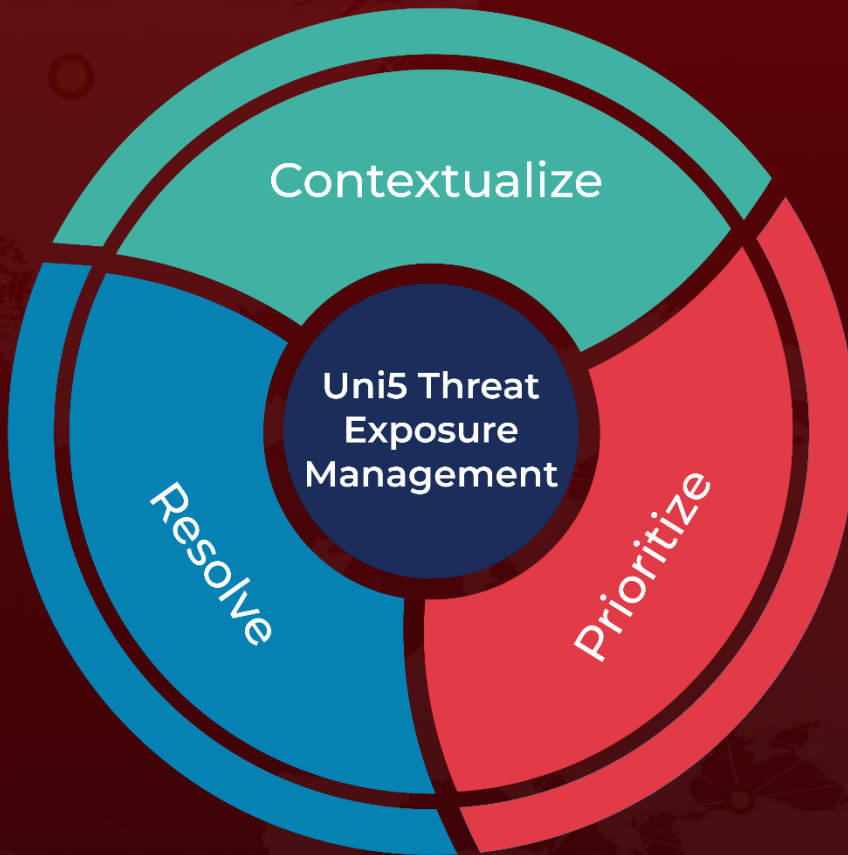
## References

<https://github.com/carsonchan12345/CVE-2024-37726-MSI-Center-Local-Privilege-Escalation>

# 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

**July 4, 2024 • 6:00 AM**

© 2024 All Rights are Reserved by Hive Pro



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