

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Microsoft's October Patch Tuesday Addresses Active Zero-Day Exploits

Date of Publication

October 10, 2024

Admiralty Code

A1

TA Number

TA2024387
















# Summary






















**First Seen:** October 8, 2024

**Affected Platforms:** Microsoft Windows, Windows Common Log File System Driver, Microsoft Office, Microsoft Azure, Microsoft Outlook, Microsoft Visual Studio

**Impact:** Denial of Service (DoS), Elevation of Privilege (EoP), Remote Code Execution (RCE), Information Disclosure, Spoofing, Security Feature Bypass, and Tampering

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-43573	Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows			
CVE-2024-43572	Microsoft Management Console Remote Code Execution Vulnerability	Microsoft Windows			
CVE-2024-6197	Open Source Curl Remote Code Execution Vulnerability	Microsoft Windows			
CVE-2024-20659	Windows Hyper-V Security Feature Bypass Vulnerability	Microsoft Windows			
CVE-2024-43583	Winlogon Elevation of Privilege Vulnerability	Microsoft Windows			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-43502	Windows Kernel Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2024-43509	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2024-43556	Windows Graphics Component Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2024-43560	Microsoft Windows Storage Port Driver Elevation of Privilege Vulnerability	Microsoft Windows			
CVE-2024-43581	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	Microsoft Windows			
CVE-2024-43609	Microsoft Office Spoofing Vulnerability	Microsoft Office			
CVE-2024-43615	Microsoft OpenSSH for Windows Remote Code Execution Vulnerability	Microsoft Windows			

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-43468	Microsoft Configuration Manager Remote Code Execution Vulnerability	Microsoft Configuration Manager	✗	✗	✓
CVE-2024-43488	Visual Studio Code extension for Arduino Remote Code Execution Vulnerability	Microsoft Visual Studio	✗	✗	✗
CVE-2024-43582	Remote Desktop Protocol Server Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓

# Vulnerability Details

## #1

Microsoft's October 2024 Patch Tuesday includes security updates for a total of 117 vulnerabilities, comprising 3 critical, 113 important, and 1 moderate-severity vulnerability. The breakdown of these vulnerabilities includes 43 Remote Code Execution, 28 Elevation of Privilege, 26 Denial of Service, 7 Security Feature Bypass, 6 Information Disclosure, 6 Spoofing, and 1 Tampering vulnerability.

## #2

The updates cover a wide range of Microsoft products, such as Windows, Office, .NET, Visual Studio, Azure, Copilot, Windows Remote Desktop, Windows Hyper-V, Windows MSHTML Platform, and other components. Notably, Microsoft also patched four non-Microsoft vulnerabilities, including one assigned to Windows by HackerOne and three affecting the Chromium-based Microsoft Edge browser, bringing the total number of CVEs to 121. This advisory pertains to 15 CVEs that could potentially be exploited.

## #3

The update addresses two zero-day vulnerabilities that are actively being exploited in the wild and three that have been publicly disclosed. This extensive patch cycle aims to address critical issues and enhance overall system security.

## #4

The two actively exploited zero-days addressed in this update are particularly concerning. The first, CVE-2024-43573, is a Windows MSHTML Platform Spoofing Vulnerability that affects the MSHTML platform still present in Windows. This flaw allows attackers to spoof file extensions in alerts when opening files.

## #5

The second actively exploited vulnerability, CVE-2024-43572, relates to Microsoft Management Console and allows malicious MSC files to execute arbitrary code on vulnerable systems. To mitigate this risk, Microsoft has implemented measures to prevent untrusted MSC files from being opened.

## #6

In addition to these actively exploited vulnerabilities, there are three publicly disclosed flaws that have not yet been exploited in the wild. These include CVE-2024-20659, a Windows Hyper-V Security Feature Bypass; CVE-2024-43583, a Winlogon Elevation of Privilege vulnerability; and CVE-2024-6197, an Open Source Curl RCE Vulnerability. While Windows does not ship the libcurl library but only ships the curl command-line tool, this vulnerability requires user interaction with a malicious server for exploitation.

## #7

Other notable vulnerabilities include multiple Elevation of Privilege flaws in the Windows Kernel and Graphics Components, Azure CLI, Monitor, Stack, Microsoft Office, SharePoint, and other products, which could grant attackers SYSTEM privileges upon exploitation. The October Patch Tuesday highlights the need for timely patching to mitigate these risks, especially those being actively exploited, ensuring system integrity and protection.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-43573	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-79
CVE-2024-43572	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-707

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-6197	CBL Mariner Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:a:haxx:libcurl:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-590
CVE-2024-20659	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:a:microsoft:office:*:*:*:*:* cpe:2.3:o:microsoft:project:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*	CWE-20
CVE-2024-43583	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-250
CVE-2024-43502	Windows 10 Windows Server 2019	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-908
CVE-2024-43509	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-416
CVE-2024-43556	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-416
CVE-2024-43560	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*	CWE-122

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-43581	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-73
CVE-2024-43609	Microsoft Office 2016 & 2019 Microsoft Office LTSC 2021 & 2024 Microsoft 365 Apps for Enterprise	cpe:2.3:a:microsoft:office:*:*:*:*:*:* cpe:2.3:a:microsoft:365_apps:*:*:*:*:*:*	CWE-200
CVE-2024-43615	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-73
CVE-2024-43468	Microsoft Configuration Manager: 2303, 2309, 2403	cpe:2.3:a:microsoft:configuration_manager:*:*:*:*:*	CWE-89
CVE-2024-43488	Microsoft Visual Studio Code: All versions	cpe:2.3:a:microsoft:vscode:*:*:*:*:*:*	CWE-306
CVE-2024-43582	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-416

# Recommendations



Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential **patches** or adopting security measures.



Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.



Prioritize patching actively exploited vulnerabilities CVE-2024-43573 and CVE-2024-43572, along with the publicly disclosed CVE-2024-6197, CVE-2024-20659, and CVE-2024-43583. These vulnerabilities have the potential for severe exploitation and should be addressed urgently.



Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.



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.

## Potential **MITRE ATT&CK TTPs**

<b>TA0004</b> Privilege Escalation	<b>TA0042</b> Resource Development	<b>TA0040</b> Impact	<b>TA0002</b> Execution
<b>TA0008</b> Lateral Movement	<b>TA0001</b> Initial Access	<b>T1588</b> Obtain Capabilities	<b>T1588.005</b> Exploits
<b>T1059</b> Command and Scripting Interpreter	<b>T1588.006</b> Vulnerabilities	<b>T1068</b> Exploitation for Privilege Escalation	<b>T1203</b> Exploitation for Client Execution
<b>T1498</b> Network Denial of Service	<b>T1566</b> Phishing	<b>T1204</b> User Execution	<b>T1210</b> Exploitation of Remote Services



## Patch Links

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-6197>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20659>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43583>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43502>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43509>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43556>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43560>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43581>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43609>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43615>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43582>

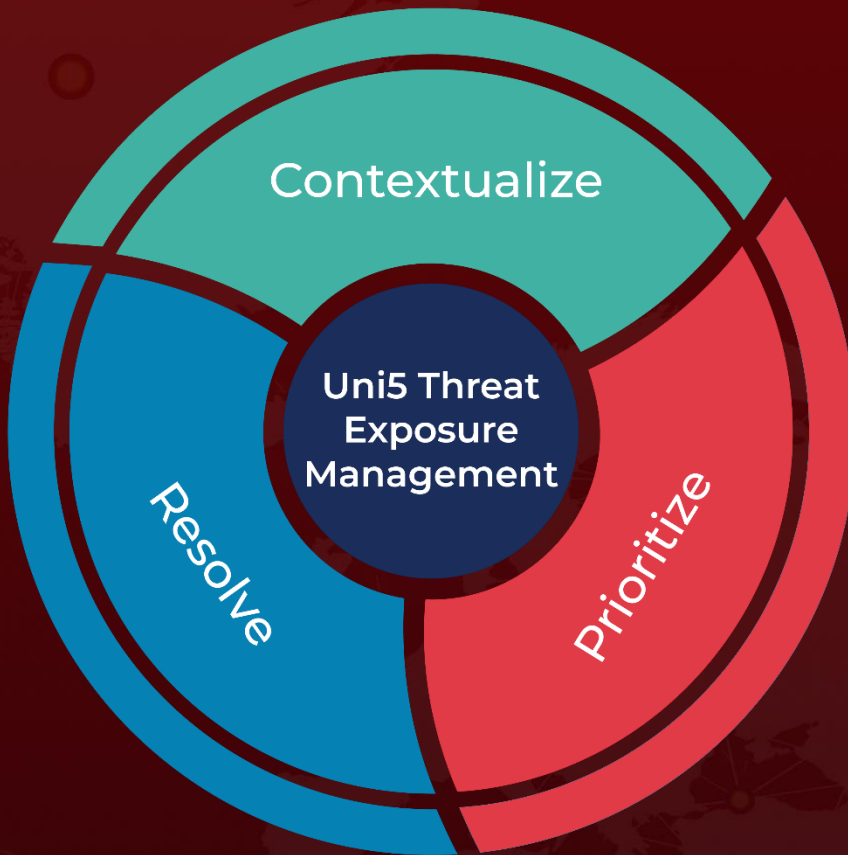
## References

<https://msrc.microsoft.com/update-guide/releaseNote/2024-oct>

# 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

**October 10, 2024 • 4:30 AM**

© 2024 All Rights are Reserved by Hive Pro



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