

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Microsoft's July Patch Tuesday Addresses Active Zero-Day Exploits

Date of Publication

July 10, 2024

Admiralty Code

A1

TA Number

TA2024267



















Summary

First Seen: July 9, 2024

Affected Products: Microsoft Exchange Server, Microsoft Office, Windows Win32K, Windows MSHTML, Windows Hyper-V, Windows Internet Connection Sharing (ICS), Windows Graphics Component

Impact: Elevation of Privilege (EoP), Remote Code Execution (RCE), Spoofing, Denial of Service (DoS)

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38080	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Hyper-V			
CVE-2024-38112	Windows MSHTML Platform Spoofing Vulnerability	Windows MSHTML			
CVE-2024-38053	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability	Windows Internet Connection Sharing (ICS)			
CVE-2024-38023	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft SharePoint Server			
CVE-2024-38060	Windows Imaging Component Remote Code Execution Vulnerability	Windows Imaging Component			
CVE-2024-38076	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Microsoft Windows			

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-38059	Win32k Elevation of Privilege Vulnerability	Windows Win32K	✗	✗	✓
CVE-2024-38066	Windows Win32k Elevation of Privilege Vulnerability	Windows Win32K	✗	✗	✓
CVE-2024-38021	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	✗	✗	✓
CVE-2024-38100	Windows File Explorer Elevation of Privilege Vulnerability	Windows File Explorer	✗	✗	✓
CVE-2024-38099	Windows Remote Desktop Licensing Service Denial of Service Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38074	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38077	Windows Remote Desktop Licensing Service Remote Code Execution Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2024-38079	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Graphics Component	✗	✗	✓
CVE-2024-38085	Windows Graphics Component Elevation of Privilege Vulnerability	Windows Graphics Component	✗	✗	✓

Vulnerability Details

#1

Microsoft's July 2024 Patch Tuesday delivers security updates for 142 vulnerabilities, including two zero-day exploits actively in the wild. The vulnerabilities addressed encompass 59 Remote Code Execution (RCE) flaws, 26 Elevation of Privilege (EoP) flaws, 24 Security Feature Bypass flaws, 17 Denial of Service (DoS) flaws, 9 Information Disclosure flaws, and 7 Spoofing flaws.

#2

These updates cover a broad range of Microsoft products, including Microsoft Exchange Server, Microsoft Office, Windows Win32K, Windows MSHTML, Windows Hyper-V, Windows Internet Connection Sharing (ICS), Windows Graphics Component, and more. Additionally, Microsoft addressed four non-Microsoft vulnerabilities: one reported by CERT/CC and Arm each, and two GitHub-assigned vulnerabilities in Active Directory.

#3

This advisory pertains to two zero-days and thirteen other vulnerabilities that have the potential for exploitation. Notably, CVE-2024-38080 has already been exploited in the wild. This EoP vulnerability in Windows Hyper-V allows an attacker to gain SYSTEM privileges. A local, authenticated attacker could leverage this flaw to escalate privileges to the SYSTEM level after initially compromising the target system.

#4

CVE-2024-38112, another zero-day, is located in Windows MSHTML. An attacker would need to send a malicious file to the victim, who must then execute it. CVE-2024-38053, a use-after-free vulnerability in the Windows Layer-2 Bridge Network Driver, allows a remote attacker on the local network to execute arbitrary code on the target system, potentially compromising a vulnerable system.

#5

Two critical vulnerabilities are deemed more likely to be exploited. CVE-2024-38023 is an RCE flaw in Microsoft SharePoint Server, where an authenticated attacker with Site Owner permissions can execute arbitrary code within the context of the SharePoint Server. CVE-2024-38060 is an RCE vulnerability in the Microsoft Windows Codecs Library that can be exploited by an authenticated attacker uploading a specially crafted malicious TIFF file.

#6

Furthermore, CVE-2024-38059 and CVE-2024-38066 are EoP vulnerabilities affecting Windows Win32k, a core kernel-side driver in Windows. These vulnerabilities can be exploited by attackers as part of post-compromise activities to escalate privileges to the SYSTEM level.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38080	Windows Server: before 2022 10.0.20348.2582 Windows: before 11 23H2 10.0.22631.3880	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *	CWE-190
CVE-2024-38112	Microsoft Internet Explorer: 11 - 11.1790.17763.0 Windows: before 11 23H2 10.0.22631.3880 Windows Server: before 2022 10.0.20348.2582	cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *	CWE-668
CVE-2024-38053	Windows: before 11 23H2 10.0.22631.3880 Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *	CWE-416
CVE-2024-38023	Microsoft SharePoint Server: 2019 Microsoft SharePoint Server Subscription Edition: All versions Microsoft SharePoint Enterprise Server: 2016	cpe:2.3:a:microsoft:sharepoint_server:-:*:*:*:*:*:*	CWE-502
CVE-2024-38060	Windows: before 11 23H2 10.0.22631.3880 Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *	CWE-122
CVE-2024-38076	Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *	CWE-122
CVE-2024-38059	Windows Server: before 2022 10.0.20348.2582 Windows: before 11 23H2 10.0.22631.3880	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *	CWE-416

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38066	Windows: before 10 1809 10.0.17763.6054 Windows Server: before 2016 10.0.14393.7159	cpe:2.3:o:microsoft:wind ows:*.~*.~*.~*.~*.~*.~* cpe:2.3:o:microsoft:wind ows_server:*.~*.~*.~*.~*.~* *	CWE-416
CVE-2024-38021	Microsoft Office: 2016 - 2019 Microsoft Office LTSC 2021: 32 bit editions - 64 bit editions Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	cpe:2.3:a:microsoft:offic e:-.~*.~*.~*.~*.~*.~* cpe:2.3:a:microsoft:365_ apps:-.~*.~*.~*.~*.~*.~*	CWE-20
CVE-2024-38100	Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:wind ows_server:*.~*.~*.~*.~*.~* *	CWE-284
CVE-2024-38099	Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:wind ows_server:*.~*.~*.~*.~*.~* *	CWE-287
CVE-2024-38074	Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:wind ows_server:*.~*.~*.~*.~*.~* *	CWE-191
CVE-2024-38077	Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:wind ows_server:*.~*.~*.~*.~*.~* *	CWE-122
CVE-2024-38079	Windows: before 11 23H2 10.0.22631.3880 Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:wind ows:*.~*.~*.~*.~*.~*.~* cpe:2.3:o:microsoft:wind ows_server:*.~*.~*.~*.~*.~* *	CWE-122
CVE-2024-38085	Windows: before 11 23H2 10.0.22631.3880 Windows Server: before 2022 10.0.20348.2582	cpe:2.3:o:microsoft:wind ows:*.~*.~*.~*.~*.~*.~* cpe:2.3:o:microsoft:wind ows_server:*.~*.~*.~*.~*.~* *	CWE-416

Recommendations



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.



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 other security measures.



Exercise meticulous surveillance on any security-related events that occur within devices and applications. If any abnormalities are discovered, take prompt action to begin the incident management procedure.



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

<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation	<u>TA0005</u> Defense Evasion	<u>TA0042</u> Resource Development
<u>TA0040</u> Impact	<u>T1203</u> Exploitation for Client Execution	<u>T1059</u> Command and Scripting Interpreter	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1040</u> Network Sniffing
<u>T1498</u> Network Denial of Service	<u>T1204</u> User Execution	<u>T1133</u> External Remote Services	<u>T1562</u> Impair Defenses
<u>T1190</u> Exploit Public-Facing Application			

Patch Links

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38053>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38023>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38060>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38076>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38059>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38066>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38021>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38100>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38099>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38074>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38077>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38079>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-38085>

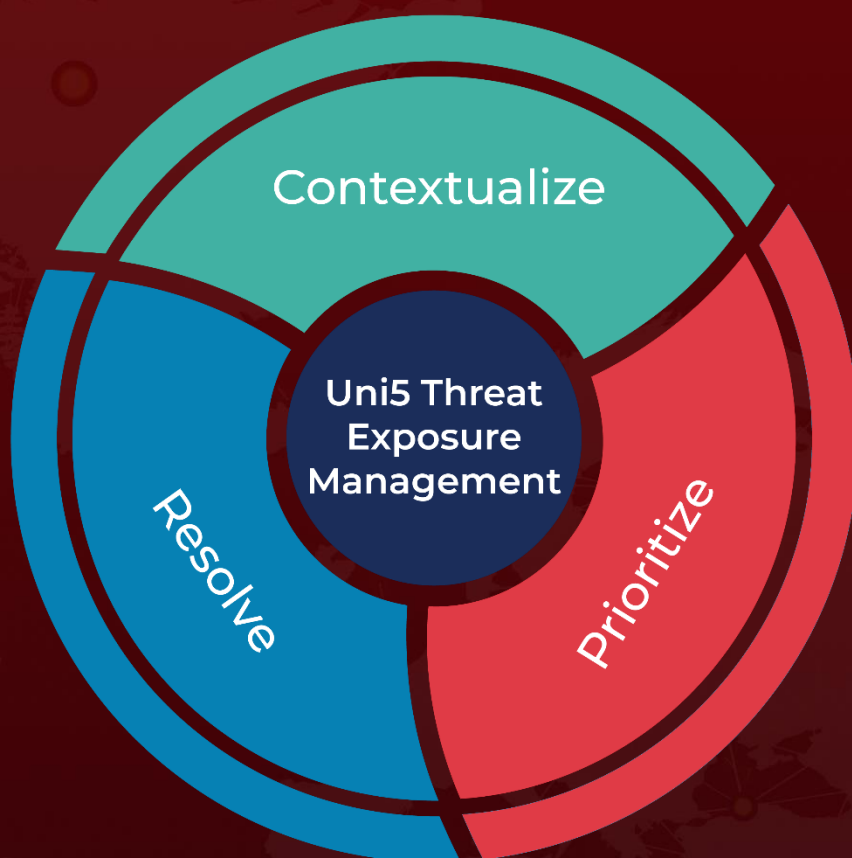
References

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

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 10, 2024 • 10:00 PM

© 2024 All Rights are Reserved by HivePro



More at www.hivepro.com