

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Microsoft's June 2024 Patch Tuesday Addresses 49 Vulnerabilities

Date of Publication

June 12, 2024

Admiralty Code

A1

TA Number

TA2024228
















Summary

First Seen: June 11, 2024

Affected Platforms: Microsoft Windows, Windows Common Log File System Driver, Microsoft Streaming Service, Win32 Kernel, Windows Cloud Files Mini Filter Driver, Microsoft Message Queuing (MSMQ), Microsoft Outlook

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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-30080	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Microsoft Message Queuing (MSMQ)			
CVE-2024-30082	Win32k Elevation of Privilege Vulnerability	Windows Win32K			
CVE-2024-30084	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	Windows Kernel-Mode Driver			
CVE-2024-30085	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver			
CVE-2024-30086	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Windows Win32 Kernel			

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-30087	Win32k Elevation of Privilege Vulnerability	Windows Win32K			
CVE-2024-30088	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel			
CVE-2024-30089	Microsoft Streaming Service Elevation of Privilege Vulnerability	Microsoft Streaming Service			
CVE-2024-30091	Win32k Elevation of Privilege Vulnerability	Windows Win32K			
CVE-2024-30099	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel			
CVE-2024-35250	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	Windows Kernel-Mode Driver			
CVE-2023-50868	NSEC3 Closest Encloser Proof DoS Vulnerability	Microsoft Windows			
CVE-2024-30103	Microsoft Outlook Remote Code Execution Vulnerability	Microsoft Outlook			

Vulnerability Details

#1

Microsoft's June 2024 Patch Tuesday includes security updates for a total of 49 vulnerabilities, comprising one critical and 48 important severity vulnerabilities. The breakdown of vulnerabilities includes 24 Elevation of Privilege, 18 Remote Code Execution, 3 Information Disclosure, and 4 Denial of Service vulnerabilities.

#2

The updates span multiple Microsoft products such as Windows, SharePoint Server, Windows Common Log File System Driver, Windows Win32k, Win32 Kernel, Visual Studio, Azure, Microsoft Outlook, and more. Notably, Microsoft patched nine non-Microsoft vulnerabilities, including one MITRE-assigned Windows vulnerability, one GitHub-assigned Visual Studio vulnerability, and six Chrome-assigned Chromium-based Microsoft Edge browser vulnerabilities, bringing the total number of CVEs to 58. This advisory pertains to 13 CVEs that could potentially be exploited.

#3

The update addresses one publicly known zero-day vulnerability, CVE-2023-50868, which was disclosed and affects DNSSEC validation. This flaw could be exploited by attackers to manipulate standard DNSSEC protocols, causing a denial of service for legitimate users by exhausting resources on a resolver.

#4

Another significant vulnerability, CVE-2024-30080, was identified in Microsoft Message Queuing (MSMQ), posing a risk of remote code execution. Attackers could achieve this by sending a malicious MSMQ packet to an MSMQ server, thereby gaining control over the server remotely.

#5

Additionally, a critical RCE vulnerability, CVE-2024-30103, in Outlook allows attackers to remotely execute code (RCE) simply by sending a malicious email. Opening the email is enough for exploitation, even without user interaction, making it particularly dangerous.

#6

Microsoft released patches for numerous vulnerabilities, including elevation of privilege risks in Win32k, the Windows Kernel-Mode Driver, and other components like the Windows Cloud Files Mini Filter Driver. These vulnerabilities could grant attackers SYSTEM privileges upon successful exploitation, highlighting the importance of promptly applying patches to enhance system security.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-30080	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-2024-30082	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-2024-30084	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-367
CVE-2024-30085	Windows: 10 - 11 23H2 Windows Server: 2019 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-122
CVE-2024-30086	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-416
CVE-2024-30087	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-20
CVE-2024-30088	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	CWE-367

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-30089	Windows: 10 - 11 23H2 Windows Server: 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	CWE-416
CVE-2024-30091	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	CWE-122
CVE-2024-30099	Windows: 10 - 11 23H2 Windows Server: 2016 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	CWE-367
CVE-2024-35250	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	CWE-822
CVE-2023-50868	Windows Server: 2012 - 2022 23H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*	CWE-400
CVE-2024-30103	Microsoft Office: 2019 Microsoft Outlook: 2016 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:outlook:*:*:*:*:*:*	CWE-184

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 critical vulnerabilities, especially CVE-2024-30080 (Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability) and CVE-2023-50868 (NSEC3 closest enclosure proof can exhaust CPU Vulnerability). 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

TA0004 Privilege Escalation	TA0042 Resource Development	TA0040 Impact	TA0002 Execution
TA0005 Defense Evasion	T1498 Network Denial of Service	T1588 Obtain Capabilities	T1588.005 Exploits
T1059 Command and Scripting Interpreter	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation	T1203 Exploitation for Client Execution

Patch Details

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30082>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30084>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30085>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30086>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30087>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30088>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30089>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30091>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30099>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35250>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-50868>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103>

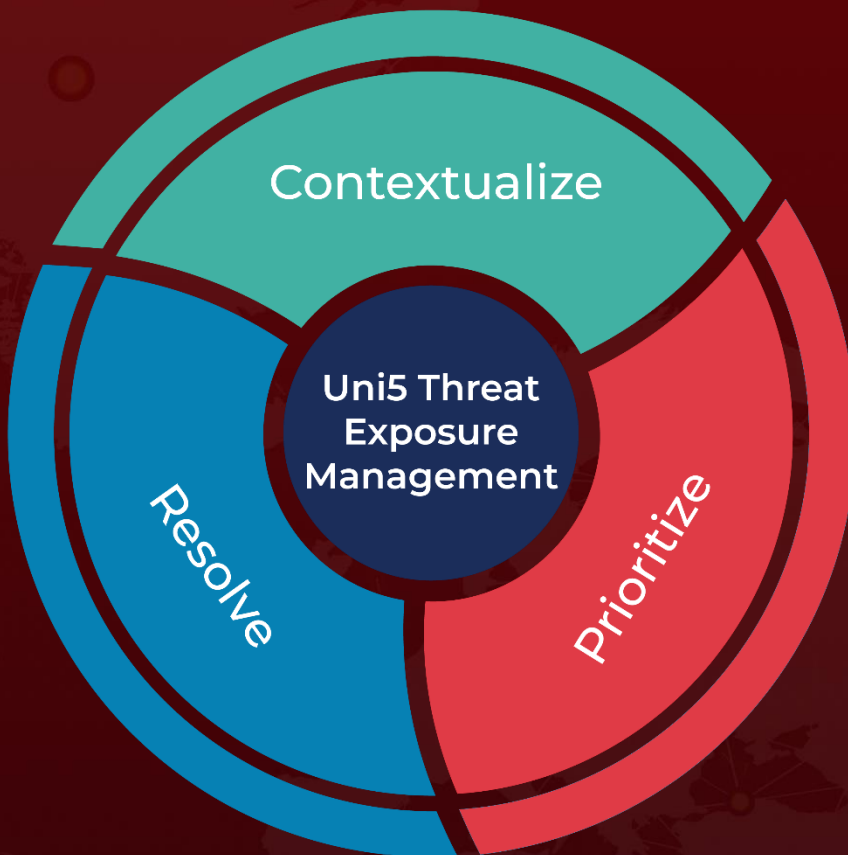
References

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

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 12, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com