

## Advisory for Microsoft Security Update

### A. Description:

Microsoft's November 2024 Patch Tuesday introduces 89 security updates, addressing critical vulnerabilities across various products. Four zero-day vulnerabilities were identified, with two actively exploited in attacks. This release includes patches for four critical flaws, focusing on remote code execution and elevation of privilege vulnerabilities. Among the fixed issues are 26 elevation of privilege vulnerabilities, 52 remote code execution vulnerabilities, four denial of service vulnerabilities, and more. Noteworthy CVEs include CVE-2024-43498, affecting .NET and Visual Studio, and CVE-2024-49056, related to Airlift. Products impacted range from Microsoft SQL Server to Windows Secure Kernel Mode, underscoring the need for prompt patching.

- 26 Elevation of Privilege vulnerabilities
- 2 Security Feature Bypass vulnerabilities
- 52 Remote Code Execution vulnerabilities
- 1 Information Disclosure vulnerability
- 4 Denial of Service vulnerabilities
- 3 Spoofing vulnerabilities

### B. CVE Details:

Tag	CVE ID	CVE Title	Severity
.NET and Visual Studio	CVE-2024-43499	.NET and Visual Studio Denial of Service Vulnerability	Important
.NET and Visual Studio	CVE-2024-43498	.NET and Visual Studio Remote Code Execution Vulnerability	Critical
Airlift.microsoft.com	CVE-2024-49056	Airlift.microsoft.com Elevation of Privilege Vulnerability	Critical
Azure CycleCloud	CVE-2024-43602	Azure CycleCloud Remote Code Execution Vulnerability	Important

LightGBM	CVE-2024-43598	LightGBM Remote Code Execution Vulnerability	Important
Microsoft Defender for Endpoint	CVE-2024-5535	OpenSSL: CVE-2024-5535 SSL_select_next_proto buffer overread	Important
Microsoft Edge (Chromium-based)	CVE-2024-10826	Chromium: CVE-2024-10826 Use after free in Family Experiences	Unknown
Microsoft Edge (Chromium-based)	CVE-2024-10827	Chromium: CVE-2024-10827 Use after free in Serial	Unknown
Microsoft Exchange Server	CVE-2024-49040	Microsoft Exchange Server Spoofing Vulnerability	Important
Microsoft Graphics Component	CVE-2024-49031	Microsoft Office Graphics Remote Code Execution Vulnerability	Important
Microsoft Graphics Component	CVE-2024-49032	Microsoft Office Graphics Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2024-49029	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2024-49026	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2024-49027	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2024-49028	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office Excel	CVE-2024-49030	Microsoft Excel Remote Code Execution Vulnerability	Important
Microsoft Office SharePoint	ADV240001	Microsoft SharePoint Server Defense in Depth Update	None
Microsoft Office Word	CVE-2024-49033	Microsoft Word Security Feature Bypass Vulnerability	Important
Microsoft PC Manager	CVE-2024-49051	Microsoft PC Manager Elevation of Privilege Vulnerability	Important
Microsoft Virtual Hard Drive	CVE-2024-38264	Microsoft Virtual Hard Disk (VHDX) Denial of Service Vulnerability	Important
Microsoft Windows DNS	CVE-2024-43450	Windows DNS Spoofing Vulnerability	Important
Role: Windows Active Directory Certificate Services	CVE-2024-49019	Active Directory Certificate Services Elevation of Privilege Vulnerability	Important
Role: Windows Hyper-V	CVE-2024-43633	Windows Hyper-V Denial of Service Vulnerability	Important
Role: Windows Hyper-V	CVE-2024-43624	Windows Hyper-V Shared Virtual Disk Elevation of Privilege Vulnerability	Important
SQL Server	CVE-2024-48998	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-48997	SQL Server Native Client Remote Code Execution Vulnerability	Important

SQL Server	CVE-2024-48993	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49001	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49000	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-48999	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49043	Microsoft.SqlServer.XEvent.Configuration.dll Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-43462	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-48995	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-48994	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-38255	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-48996	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-43459	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49002	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49013	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49014	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49011	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49012	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49015	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49018	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49021	Microsoft SQL Server Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49016	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49017	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49010	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49005	SQL Server Native Client Remote Code Execution Vulnerability	Important

SQL Server	CVE-2024-49007	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49003	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49004	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49006	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49009	SQL Server Native Client Remote Code Execution Vulnerability	Important
SQL Server	CVE-2024-49008	SQL Server Native Client Remote Code Execution Vulnerability	Important
TorchGeo	CVE-2024-49048	TorchGeo Remote Code Execution Vulnerability	Important
Visual Studio	CVE-2024-49044	Visual Studio Elevation of Privilege Vulnerability	Important
Visual Studio Code	CVE-2024-49050	Visual Studio Code Python Extension Remote Code Execution Vulnerability	Important
Visual Studio Code	CVE-2024-49049	Visual Studio Code Remote Extension Elevation of Privilege Vulnerability	Moderate
Windows CSC Service	CVE-2024-43644	Windows Client-Side Caching Elevation of Privilege Vulnerability	Important
Windows Defender Application Control (WDAC)	CVE-2024-43645	Windows Defender Application Control (WDAC) Security Feature Bypass Vulnerability	Important
Windows DWM Core Library	CVE-2024-43636	Win32k Elevation of Privilege Vulnerability	Important
Windows DWM Core Library	CVE-2024-43629	Windows DWM Core Library Elevation of Privilege Vulnerability	Important
Windows Kerberos	CVE-2024-43639	Windows Kerberos Remote Code Execution Vulnerability	Critical
Windows Kernel	CVE-2024-43630	Windows Kernel Elevation of Privilege Vulnerability	Important
Windows NT OS Kernel	CVE-2024-43623	Windows NT OS Kernel Elevation of Privilege Vulnerability	Important
Windows NTLM	CVE-2024-43451	NTLM Hash Disclosure Spoofing Vulnerability	Important
Windows Package Library Manager	CVE-2024-38203	Windows Package Library Manager Information Disclosure Vulnerability	Important
Windows Registry	CVE-2024-43641	Windows Registry Elevation of Privilege Vulnerability	Important
Windows Registry	CVE-2024-43452	Windows Registry Elevation of Privilege Vulnerability	Important
Windows Secure Kernel Mode	CVE-2024-43631	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	Important

Windows Secure Kernel Mode	CVE-2024-43646	Windows Secure Kernel Mode Elevation of Privilege Vulnerability	Important
Windows Secure Kernel Mode	CVE-2024-43640	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	Important
Windows SMB	CVE-2024-43642	Windows SMB Denial of Service Vulnerability	Important
Windows SMBv3 Client/Server	CVE-2024-43447	Windows SMBv3 Server Remote Code Execution Vulnerability	Important
Windows Task Scheduler	CVE-2024-49039	Windows Task Scheduler Elevation of Privilege Vulnerability	Important
Windows Telephony Service	CVE-2024-43628	Windows Telephony Service Remote Code Execution Vulnerability	Important
Windows Telephony Service	CVE-2024-43621	Windows Telephony Service Remote Code Execution Vulnerability	Important
Windows Telephony Service	CVE-2024-43620	Windows Telephony Service Remote Code Execution Vulnerability	Important
Windows Telephony Service	CVE-2024-43627	Windows Telephony Service Remote Code Execution Vulnerability	Important
Windows Telephony Service	CVE-2024-43635	Windows Telephony Service Remote Code Execution Vulnerability	Important
Windows Telephony Service	CVE-2024-43622	Windows Telephony Service Remote Code Execution Vulnerability	Important
Windows Telephony Service	CVE-2024-43626	Windows Telephony Service Elevation of Privilege Vulnerability	Important
Windows Update Stack	CVE-2024-43530	Windows Update Stack Elevation of Privilege Vulnerability	Important
Windows USB Video Driver	CVE-2024-43643	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	Important
Windows USB Video Driver	CVE-2024-43449	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	Important
Windows USB Video Driver	CVE-2024-43637	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	Important
Windows USB Video Driver	CVE-2024-43634	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	Important
Windows USB Video Driver	CVE-2024-43638	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	Important
Windows VMSwitch	CVE-2024-43625	Microsoft Windows VMSwitch Elevation of Privilege Vulnerability	Critical
Windows Win32 Kernel Subsystem	CVE-2024-49046	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Important

### C. Reference:

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