Reference	Description	Additional Information	Vendor Severity	CVSS Severity	Publicly Aware	Weaponised	Countermeasure	Impact	Exploitability Assessment
CVE-2025-24985	Windows Fast FAT File System Driver Remote Code Execution Vulnerability	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally.	Important	7.8	No	Yes	No	Remote Code Execution	Exploitation Detected
CVE-2025-24993	Windows NTFS Remote Code Execution Vulnerability	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	Important	7.8	No	Yes	No	Remote Code Execution	Exploitation Detected
CVE-2025-24983	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	7.0	No	Yes	No	Elevation of Privilege	Exploitation Detected
CVE-2025-26633	Microsoft Management Console Security Feature Bypass Vulnerability	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally.	Important	7.0	No	Yes	No	Security Feature Bypass	Exploitation Detected
CVE-2025-24991	Windows NTFS Information Disclosure Vulnerability	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory.	Important	5.5	No	Yes	No	Information Disclosure	Exploitation Detected
CVE-2025-24984	Windows NTFS Information Disclosure Vulnerability	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. An attacker who successfully exploited this vulnerability could potentially read portions of heap memory.	Important	4.6	No	Yes	No	Information Disclosure	Exploitation Detected
CVE-2025-26630	Microsoft Access Remote Code Execution Vulnerability	Use after free in Microsoft Office Access allows an unauthorized attacker to execute code locally. No, the Preview Pane is not an attack vector.	Important	7.8	Yes	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-26645	Remote Desktop Client Remote Code Execution Vulnerability	Relative path traversal in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	Critical	8.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24051	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to execute code over a network.	Important	8.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24056	Windows Telephony Service Remote Code Execution Vulnerability	Heap-based buffer overflow in Windows Telephony Server allows an unauthorized attacker to execute code over a network.	Important	8.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24084	Windows Subsystem for Linux (WSL2) Kernel Remote Code Execution Vulnerability	Untrusted pointer dereference in Windows Subsystem for Linux allows an unauthorized attacker to execute code locally.	Critical	8.4	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24066	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Use after free in Microsoft Streaming Service allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	8.4	No	No	No	Elevation of Privilege	Exploitation More Likely
CVE-2025-24035	Windows Remote Desktop Services Remote Code Execution Vulnerability	Sensitive data storage in improperly locked memory in Windows Remote Desktop Services allows an unauthorized attacker to execute code over a network.	Critical	8.1	No	No	No	Remote Code Execution	Exploitation More Likely
CVE-2025-24045	Windows Remote Desktop Services Remote Code Execution Vulnerability	Sensitive data storage in improperly locked memory in Windows Remote Desktop Services allows an unauthorized attacker to execute code over a network.	Critical	8.1	No	No	No	Remote Code Execution	Exploitation More Likely
CVE-2025-24064	Windows Domain Name Service Remote Code Execution Vulnerability	Use after free in DNS Server allows an unauthorized attacker to execute code over a network.	Critical	8.1	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24057	Microsoft Office Remote Code Execution Vulnerability	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	Critical	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-21180	Windows exFAT File System Remote Code Execution Vulnerability	Heap-based buffer overflow in Windows exFAT File System allows an unauthorized attacker to execute code locally.	Important	7.8	No	No	No	Remote Code Execution	Exploitation More Likely
CVE-2025-24044	Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges	Important	7.8	No	No	No	Elevation of Privilege	Exploitation More Likely
CVE-2025-24046	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Use after free in Microsoft Streaming Service allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	7.8	No	No	No	Elevation of Privilege	Exploitation Less Likely

CVE-2025-24048	Windows Hyper-V Elevation of Privilege Vulnerability	Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain Kernel Memory Access.	Important	7.8	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24050	Windows Hyper-V Elevation of Privilege Vulnerability	Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain Kernel Memory Access.	Important	7.8	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24059	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Incorrect conversion between numeric types in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	Important	7.8	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24061	Windows Mark of the Web Security Feature Bypass Vulnerability	Protection mechanism failure in Windows Mark of the Web (MOTW) allows an unauthorized attacker to bypass a security feature locally. An attacker who successfully exploited the vulnerability could evade Mark of the Web (MOTW) defenses.	Important	7.8	No	No	No	Security Feature Bypass	Exploitation More Likely
CVE-2025-24067	Kernel Streaming Service Driver Elevation of Privilege Vulnerability	Use after free in Microsoft Streaming Service allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	7.8	No	No	No	Elevation of Privilege	Exploitation More Likely
CVE-2025-24072	Microsoft Local Security Authority (LSA) Server Elevation of Privilege Vulnerability	Use after free in Microsoft Local Security Authority Server (lsasrv) allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	7.8	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24075	Microsoft Excel Remote Code Execution Vulnerability	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally. The Preview Pane is not an attack vector	Important	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24077	Microsoft Word Remote Code Execution Vulnerability	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally. The Preview Pane is not an attack vector.	Important	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24079	Microsoft Word Remote Code Execution Vulnerability	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally. The Preview Pane is not an attack vector.	Important	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24080	Microsoft Office Remote Code Execution Vulnerability	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally. The Preview Pane is not an attack vector.	Important	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24081	Microsoft Excel Remote Code Execution Vulnerability	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally. No, the Preview Pane is not an attack vector.	Important	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24082	Microsoft Excel Remote Code Execution Vulnerability	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally. No, the Preview Pane is not an attack vector.	Important	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24083	Microsoft Office Remote Code Execution Vulnerability	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally. No, the Preview Pane is not an attack vector.	Important	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24995	Kernel Streaming WOW Thunk Service Driver Elevation of Privilege Vulnerability	Heap-based buffer overflow in Kernel Streaming WOW Thunk Service Driver allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	7.8	No	No	No	Elevation of Privilege	Exploitation More Likely
CVE-2025-26629	Microsoft Office Remote Code Execution Vulnerability	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally. No, the Preview Pane is not an attack vector.	Important	7.8	No	No	No	Remote Code Execution	Exploitation Less Likely

CVE-2025-24043	WinDbg Remote Code Execution Vulnerability	Improper verification of cryptographic signature in .NET allows an authorized attacker to execute code over a network.	Important	7.5	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24071	Microsoft Windows File Explorer Spoofing Vulnerability	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an unauthorized attacker to perform spoofing over a network.	Important	7.5	No	No	No	Spoofing	Exploitation Less Likely
CVE-2025-24076	Microsoft Windows Cross Device Service Elevation of Privilege Vulnerability	Improper access control in Windows Cross Device Service allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	7.3	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24994	Microsoft Windows Cross Device Service Elevation of Privilege Vulnerability	Improper access control in Windows Cross Device Service allows an authorized attacker to elevate privileges locally.	Important	7.3	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24998	Visual Studio Installer Elevation of Privilege Vulnerability	Uncontrolled search path element in Visual Studio allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain administrator privileges.	Important	7.3	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-25003	Visual Studio Elevation of Privilege Vulnerability	Uncontrolled search path element in Visual Studio allows an authorized attacker to elevate privileges locally.	Important	7.3	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-26631	Visual Studio Code Elevation of Privilege Vulnerability	Uncontrolled search path element in Visual Studio Code allows an authorized attacker to elevate privileges locally. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	7.3	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-25008	Windows Server Elevation of Privilege Vulnerability	Improper link resolution before file access ('link following') in Microsoft Windows allows an authorized attacker to elevate privileges locally. An attacker would be able to delete targeted files on a system.	Important	7.1	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24070	ASP.NET Core and Visual Studio Elevation of Privilege Vulnerability	Weak authentication in ASP.NET Core & Visual Studio allows an unauthorized attacker to elevate privileges over a network. An attacker who successfully exploited this vulnerability could gain the privileges of the compromised user.	Important	7.0	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24078	Microsoft Word Remote Code Execution Vulnerability	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally. The Preview Pane is not an attack vector.	Important	7.0	No	No	No	Remote Code Execution	Exploitation Less Likely
CVE-2025-24987	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	Out-of-bounds read in Windows USB Video Driver allows an authorized attacker to elevate privileges with a physical attack. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	6.6	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24988	Windows USB Video Class System Driver Elevation of Privilege Vulnerability	Out-of-bounds read in Windows USB Video Driver allows an authorized attacker to elevate privileges with a physical attack. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Important	6.6	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24054	NTLM Hash Disclosure Spoofing Vulnerability	External control of file name or path in Windows NTLM allows an unauthorized attacker to perform spoofing over a network.	Important	6.5	No	No	No	Spoofing	Exploitation Less Likely
CVE-2025-24996	NTLM Hash Disclosure Spoofing Vulnerability	External control of file name or path in Windows NTLM allows an unauthorized attacker to perform spoofing over a network.	Important	6.5	No	No	No	Spoofing	Exploitation Less Likely
CVE-2025-21199	Azure Agent Installer for Backup and Site Recovery Elevation of Privilege Vulnerability	Improper privilege management in Azure Agent Installer allows an authorized attacker to elevate privileges locally.	Important	5.8	No	No	No	Elevation of Privilege	Exploitation Less Likely
CVE-2025-24992	Windows NTFS Information Disclosure Vulnerability	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. An attacker who successfully exploited this vulnerability could potentially read portions of heap memory.	Important	5.5	No	No	No	Information Disclosure	Exploitation More Likely

CVE-2025-24997	DirectX Graphics Kernel File Denial of Service Vulnerability	Successful exploitation of this vulnerability requires an attacker to compromise admin credentials on the device.	Important	4.4	No	No	No	Denial of Service	Exploitation Less Likely
CVE-2025-21247	MapUrlToZone Security Feature Bypass Vulnerability	Improper resolution of path equivalence in Windows MapUrlToZone allows an unauthorized attacker to bypass a security feature over a network.	Important	4.3	No	No	No	Security Feature Bypass	Exploitation More Likely
CVE-2025-24055	Windows USB Video Class System Driver Information Disclosure Vulnerability	Out-of-bounds read in Windows USB Video Driver allows an authorized attacker to disclose information with a physical attack.	Important	4.3	No	No	No	Information Disclosure	Exploitation Less Likely