Reference	Description	Vendor Severity	CVSS Score	Weapon-ised	Publicly Aware	Counter-measure	Additional Details	Exploitability Assessment	Impact
CVE-2025-21418	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important	7.8	Yes	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation Detected	Elevation of Privilege
CVE-2025-21391	Windows Storage Elevation of Privilege Vulnerability	Important	7.1	Yes	No	No	An attacker would only be able to delete targeted files on a system.	Exploitation Detected	Elevation of Privilege
CVE-2025-21194	Microsoft Surface Security Feature Bypass Vulnerability	Important	7.1	No	Yes	No	This Hypervisor vulnerability relates to Virtual Machines within a Unified Extensible Firmware Interface (UEFI) host machine. On some specific hardware it might be possible to bypass the UEFI, which could lead to the compromise of the hypervisor and the secure kernel. Successful exploitation of this vulnerability by an attacker requires a user to first reboot their machine.	Exploitation Less Likely	Security Feature Bypass
CVE-2025-21377	NTLM Hash Disclosure Spoofing Vulnerability	Important	6.5	No	Yes	No	This vulnerability discloses a user's NTLMv2 hash to the attacker who could use this to authenticate as the user. While Microsoft has announced retirement of the Internet Explorer 11 application on certain platforms and the Microsoft Edge Legacy application is deprecated, the underlying MSHTML, EdgeHTML, and scripting platforms are still supported. The MSHTML platform is used by Internet Explorer mode in Microsoft Edge as well as other applications through WebBrowser control.	Exploitation More Likely	Spoofing
	Microsoft High						Scope = Changed, Jump Point = True		

CVE-2025-21198	Performance Compute (HPC) Pack Remote Code Execution Vulnerability	Important	9	No	No	No	An attacker could exploit this vulnerability by sending a specially crafted HTTPS request to the targeted head node or Linux node granting them the ability to perform RCE on other clusters or nodes connected to the targeted head node.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21190	Service Remote Code Execution	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21200	Service Remote Code Execution	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21201	Server Remote Code Execution	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21208	and Remote Access Service (RRAS) Remote Code	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21368	Authentication Remote Code	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21369	Authentication Remote Code	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21406	Service Remote Code Execution	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21407	Service Remote Code Execution	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21410	and Remote Access Service (RRAS) Remote Code	Important	8.8	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21371	Service Remote Code Execution Vulnerability	Important	8.8	No	No	No	This attack requires a client to connect to a malicious server, and that could allow the attacker to gain code execution on the client.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21376	Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	Critical	8.1	No	No	No	An unauthenticated attacker could send a specially crafted request to a vulnerable LDAP server. Successful exploitation could result in a buffer overflow which could be leveraged to achieve remote code execution.	Exploitation More Likely	Remote Code Execution
CVE-2025-21400	Microsoft SharePoint Server Remote Code Execution Vulnerability	Important	8	No	No	No	In a network-based attack, an authenticated attacker, as at least a Site Owner, could write arbitrary code to inject and execute code remotely on the SharePoint Server.	Exploitation More Likely	Remote Code Execution

CVE-2025-21322	Manager Elevation of Privilege	Important	7.8	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation Less Likely	Elevation of Privilege
CVE-2025-21358	Messaging Elevation of Privileges	Important	7.8	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation More Likely	Elevation of Privilege
CVE-2025-21359	Security Feature Bypass Vulnerability	Important	7.8	No	No	No	An authenticated standard user is able to bypass user access control (UAC) prompt.	Exploitation Less Likely	Feature Bypass
CVE-2025-21367	Kernel Subsystem Elevation of	Important	7.8	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation More Likely	Elevation of Privilege
CVE-2025-21375	WOW Thunk Service Driver Elevation of Privilege	Important	7.8	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation Less Likely	Elevation of Privilege
CVE-2025-21381	Remote Code Execution	Important	7.8	No	No	No	The Preview Pane is an attack vector.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21383	Information Disclosure Vulnerability	Important	7.8	No	No	No	An attacker who successfully exploited this vulnerability could potentially read small portions of heap memory.	Exploitation Less Likely	Information Disclosure
CVE-2025-21386	Remote Code Execution	Important	7.8	No	No	No	The Preview Pane is an attack vector.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21387	Remote Code Execution	Important	7.8	No	No	No	The Preview Pane is an attack vector.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21390	Remote Code Execution	Important	7.8	No	No	No	The Preview Pane is an attack vector.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21392	Remote Code Execution	Important	7.8	No	No	No	The Preview Pane is not an attack vector.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21394	Remote Code Execution	Important	7.8	No	No	No	The Preview Pane is an attack vector.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21397	Remote Code Execution	Important	7.8	No	No	No	The Preview Pane is not an attack vector.	Exploitation Less Likely	Remote Code Execution
CVE-2025-21420	Cleanup Tool Elevation of	Important	7.8	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation More Likely	Elevation of Privilege
CVE-2025-21373	Elevation of Privilege	Important	7.8	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation Less Likely	Elevation of Privilege
CVE-2025-21181	Queuing (MSMQ) Denial of Service	Important	7.5	No	No	No		Exploitation Less Likely	Denial of Service
CVE-2025-21351	Directory Domain Services API Denial of Service	Important	7.5	No	No	No		Exploitation Less Likely	Denial of Service

CVE-2025-21182	File System (ReFS) Deduplication Service Elevation of	Important	7.4	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation Less Likely	Elevation of Privilege
CVE-2025-21183	File System (ReFS) Deduplication Service Elevation of	Important	7.4	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation Less Likely	Elevation of Privilege
CVE-2025-21206	Installer Elevation of Privilege	Important	7.3	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation Less Likely	Elevation of Privilege
CVE-2025-24039	Elevation of Privilege	Important	7.3	No	No	No		Exploitation Less Likely	Elevation of Privilege
CVE-2025-24042	JS Debug Extension Elevation of Privilege	Important	7.3	No	No	No	The attacker would gain the rights of the user that is running the affected application.	Exploitation Less Likely	Elevation of Privilege
CVE-2025-21379	Remote Code Execution	Critical	7.1	No	No	No		Exploitation Less Likely	Remote Code Execution
CVE-2025-21419	Cleanup Elevation of Privilege	Important	7.1	No	No	No	An attacker would only be able to delete targeted files on a system.	Exploitation More Likely	Elevation of Privilege
CVE-2025-21184	Messaging Elevation of Privileges	Important	7	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation More Likely	Elevation of Privilege
CVE-2025-21414	Messaging Elevation of Privileges	Important	7	No	No	No	An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.	Exploitation More Likely	Elevation of Privilege
CVE-2025-24036	AutoUpdate (MAU) Elevation of	Important	7	No	No	No		Exploitation Less Likely	Elevation of Privilege
CVE-2025-21349	Desktop Configuration Service Tampering	Important	6.8	No	No	No		Exploitation Less Likely	Tampering
CVE-2025-21212	Sharing (ICS) Denial of Service	Important	6.5	No	No	No		Exploitation Less Likely	Denial of Service
CVE-2025-21216	Sharing (ICS) Denial of Service	Important	6.5	No	No	No		Exploitation Less Likely	Denial of Service
CVE-2025-21254	Sharing (ICS) Denial of Service	Important	6.5	No	No	No		Exploitation Less Likely	Denial of Service
CVE-2025-21352	Sharing (ICS) Denial of Service Vulnerability	Important	6.5	No	No	No	An attacker can send specially crafted packets which could affect availability of the service and result in Denial of Service (DoS).	Exploitation Less Likely	Denial of Service

CVE-2025-21347	Windows Deployment Services Denial of Service Vulnerability	Important	6	No	No	No	An attacker who successfully exploits this vulnerability cannot access files but can overwrite their contents and potentially cause the service to become unavailable.	Exploitation Less Likely	Denial of Service
CVE-2025-21350	Denial of Service Vulnerability	Important	5.9	No	No	No		Exploitation Less Likely	Denial of Service
CVE-2025-21179	Denial of Service Vulnerability	Important	4.8	No	No	No		Exploitation Less Likely	Denial of Service
CVE-2025-21337	Elevation of Privilege	Important	3.3	No	No	No	An attacker would only be able to list folder contents and not gain system privileges.	Exploitation Less Likely	Elevation of Privilege