Severity

High

Analysis Summary

Following are the Microsoft patch Tuesday vulnerabilities released in the month of April

CVE	Title	Severity	CVSS	Type
CVE-2022-24521	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important	7.8	EoP
CVE-2022-26904	Windows User Profile Service Elevation of Privilege Vulnerability	Important	7	EoP
CVE-2022-23259	Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability	Critical	8.8	RCE
CVE-2022-26809	RPC Runtime Library Remote Code Execution Vulnerability	Critical	9.8	RCE
CVE-2022-22008	Windows Hyper-V Remote Code Execution Vulnerability	Critical	7.7	RCE
CVE-2022-23257	Windows Hyper-V Remote Code Execution Vulnerability	Critical	8.6	RCE
CVE-2022-24537	Windows Hyper-V Remote Code Execution Vulnerability	Critical	7.7	RCE
CVE-2022-26919	Windows LDAP Remote Code Execution Vulnerability	Critical	8.1	RCE
CVE-2022-24491	Windows Network File System Remote Code Execution Vulnerability	Critical	9.8	RCE
CVE-2022-24497	Windows Network File System Remote Code Execution Vulnerability	Critical	9.8	RCE
CVE-2022-24541	Windows Server Service Remote Code Execution Vulnerability	Critical	8.8	RCE
CVE-2022-24500	Windows SMB Remote Code Execution Vulnerability	Critical	8.8	RCE
CVE-2022-26832	.NET Framework Denial of Service Vulnerability	Important	7.5	DoS
CVE-2022-26907	Azure SDK for .NET Information Disclosure Vulnerability	Important	5.3	Info
CVE-2022-26896	Azure Site Recovery Elevation of Privilege Vulnerability	Important	4.9	EoP
CVE-2022-26897	Azure Site Recovery Elevation of Privilege Vulnerability	Important	4.9	EoP
CVE-2022-26898	Azure Site Recovery Remote Code Execution Vulnerability	Important	7.2	RCE
CVE-2022-24489	Cluster Client Failover (CCF) Elevation of Privilege Vulnerability	Important	7.8	EoP
CVE-2022-24479	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability	Important	7.8	EoP
CVE-2022-26830	DiskUsage.exe Remote Code Execution Vulnerability	Important	7.5	RCE
CVE-2022-24767	GitHub: Git for Windows' uninstaller vulnerable to DLL hijacking when run under the SYSTEM user account	Important	Unknown	EoP
CVE-2022-24765	GitHub: Uncontrolled search for the Git directory in Git for Windows	Important	Unknown	EoP
CVE-2022-24532	HEVC Video Extensions Remote Code Execution Vulnerability	Important	7.8	RCE
CVE-2022-24496	Local Security Authority (LSA) Elevation of Privilege Vulnerability	Important	7.8	EoP
CVE-2022-24548	Microsoft Defender Denial of Service Vulnerability	Important	5.5	DoS
CVE-2022-24475	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Important	8.3	EoP
CVE-2022-26891	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Important	8.3	EoP
CVE-2022-26894	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Important	8.3	EoP
CVE-2022-26895	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Important	8.3	EoP
CVE-2022-26900	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Important	8.3	EoP
CVE-2022-26908	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Important	8.3	EoP
CVE-2022-24473	Microsoft Excel Remote Code Execution Vulnerability	Important	7.8	RCE
CVE-2022-26901	Microsoft Excel Remote Code Execution Vulnerability	Important	7.8	RCE
CVE-2022-26924	YARP Denial of Service Vulnerability	Important	7.5	DoS
CVE-2022-24493	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	Important	5.5	Info
CVE-2022-23292	Microsoft Power BI Spoofing Vulnerability	Important	7.1	Spoofing
CVE-2022-24472	Microsoft SharePoint Server Spoofing Vulnerability	Important	8	Spoofing

CVE-2022-26788	PowerShell Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24533	Remote Desktop Protocol Remote Code Execution Vulnerability	Important 8	RCE
CVE-2022-24492	Remote Procedure Call Runtime Remote Code Execution Vulnerability	Important 8.8	RCE
CVE-2022-24528	Remote Procedure Call Runtime Remote Code Execution Vulnerability	Important 8.8	RCE
CVE-2022-26910	Skype for Business and Lync Spoofing Vulnerability	Important 5.3	Spoofing
CVE-2022-26911	Skype for Business Information Disclosure Vulnerability	Important 6.5	Info
CVE-2022-26921	Visual Studio Code Elevation of Privilege Vulnerability	Important Unknown	EoP
CVE-2022-24513	Visual Studio Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24485	Win32 File Enumeration Remote Code Execution Vulnerability	Important 7.5	RCE
CVE-2022-21983	Win32 Stream Enumeration Remote Code Execution Vulnerability	Important 7.5	RCE
CVE-2022-24534	Win32 Stream Enumeration Remote Code Execution Vulnerability	Important 7.5	RCE
CVE-2022-26914	Win32k Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24482	Windows ALPC Elevation of Privilege Vulnerability	Important 7	EoP
CVE-2022-24540	Windows ALPC Elevation of Privilege Vulnerability	Important 7	EoP
CVE-2022-24494	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24549	Windows AppX Package Manager Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26828	Windows Bluetooth Driver Elevation of Privilege Vulnerability	Important 7	EoP
CVE-2022-24484	Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability	Important 5.5	DoS
CVE-2022-24538	Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability	Important 6.5	DoS
CVE-2022-26784	Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability	Important 6.5	DoS
CVE-2022-24481	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24488	Windows Desktop Bridge Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24547	Windows Digital Media Receiver Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24495	Windows Direct Show — Remote Code Execution Vulnerability	Important 7	RCE
CVE-2022-26816	Windows DNS Server Information Disclosure Vulnerability	Important 4.9	Info
CVE-2022-24536	Windows DNS Server Remote Code Execution Vulnerability	Important 7.2	RCE
CVE-2022-26811	Windows DNS Server Remote Code Execution Vulnerability	Important 7.2	RCE
CVE-2022-26812	Windows DNS Server Remote Code Execution Vulnerability	Important 6.7	RCE
CVE-2022-26813	Windows DNS Server Remote Code Execution Vulnerability	Important 7.2	RCE
CVE-2022-26814	Windows DNS Server Remote Code Execution Vulnerability	Important 7.5	RCE
CVE-2022-26815	Windows DNS Server Remote Code Execution Vulnerability	Important 8.8	RCE
CVE-2022-26817	Windows DNS Server Remote Code Execution Vulnerability	Important 7.5	RCE
CVE-2022-26818	Windows DNS Server Remote Code Execution Vulnerability	Important 7.5	RCE
CVE-2022-26819	Windows DNS Server Remote Code Execution Vulnerability	Important 6.6	RCE
CVE-2022-26820	Windows DNS Server Remote Code Execution Vulnerability	Important 6.6	RCE
CVE-2022-26821	Windows DNS Server Remote Code Execution Vulnerability	Important 6.6	RCE
CVE-2022-26822	Windows DNS Server Remote Code Execution Vulnerability	Important 6.6	RCE
CVE-2022-26823	Windows DNS Server Remote Code Execution Vulnerability	Important 7.2	RCE
CVE-2022-26824	Windows DNS Server Remote Code Execution Vulnerability	Important 7.2	RCE
CVE-2022-26825	Windows DNS Server Remote Code Execution Vulnerability	Important 7.2	RCE
CVE-2022-26826	Windows DNS Server Remote Code Execution Vulnerability	Important 7.2	RCE
CVE-2022-26829	Windows DNS Server Remote Code Execution Vulnerability	Important 7.5	RCE
CVE-2022-24546	Windows DWM Core Library Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24527	Windows Endpoint Configuration Manager Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26916	Windows Fax Compose Form Remote Code Execution Vulnerability	Important 7.8	RCE
CVE-2022-26917	Windows Fax Compose Form Remote Code Execution Vulnerability	Important 7.8	RCE

CVE-2022-26918	Windows Fax Compose Form Remote Code Execution Vulnerability	Important 7.8	RCE
CVE-2022-26808	Windows File Explorer Elevation of Privilege Vulnerability	Important 7	EoP
CVE-2022-26810	Windows File Server Resource Management Service Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26827	Windows File Server Resource Management Service Elevation of Privilege Vulnerability	Important 7	EoP
CVE-2022-26920	Windows Graphics Component Information Disclosure Vulnerability	Important 5.5	Info
CVE-2022-26903	Windows Graphics Component Remote Code Execution Vulnerability	Important 7.8	RCE
CVE-2022-23268	Windows Hyper-V Denial of Service Vulnerability	Important 6.5	DoS
CVE-2022-22009	Windows Hyper-V Remote Code Execution Vulnerability	Important 7.7	RCE
CVE-2022-24490	Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability	Important 8.1	Info
CVE-2022-24539	Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability	Important 8.1	Info
CVE-2022-26783	Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability	Important 6.5	Info
CVE-2022-26785	Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability	Important 6.5	Info
CVE-2022-24499	Windows Installer Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24530	Windows Installer Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24498	Windows iSCSI Target Service Information Disclosure Vulnerability	Important 6.5	Info
CVE-2022-24486	Windows Kerberos Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24544	Windows Kerberos Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24545	Windows Kerberos Remote Code Execution Vulnerability	Important 8.1	RCE
CVE-2022-24483	Windows Kernel Information Disclosure Vulnerability	Important 5.5	Info
CVE-2022-26831	Windows LDAP Denial of Service Vulnerability	Important 7.5	DoS
CVE-2022-24487	Windows Local Security Authority (LSA) Remote Code Execution Vulnerability	Important 8.8	RCE
CVE-2022-26786	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26787	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26789	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26790	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26791	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26792	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26793	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26794	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26795	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26796	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26797	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26798	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26801	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26802	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26803	Windows Print Spooler Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26915	Windows Secure Channel Denial of Service Vulnerability	Important 7.5	DoS
CVE-2022-24550	Windows Telephony Server Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24543	Windows Upgrade Assistant Remote Code Execution Vulnerability	Important 7.8	RCE
CVE-2022-24474	Windows Win32k Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-24542	Windows Win32k Elevation of Privilege Vulnerability	Important 7.8	EoP
CVE-2022-26807	Windows Work Folder Service Elevation of Privilege Vulnerability	Important 7	EoP
CVE-2022-26909	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Moderate 8.3	EoP
CVE-2022-26912	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Moderate 8.3	EoP
CVE-2022-24523	Microsoft Edge (Chromium-based) Spoofing Vulnerability	Moderate 4.3	EoP
	Chromium: Inappropriate implementation in Full Screen Mode	High N/A	RCE

CVE-2022-1129 *				
CVE-2022-1128 *	Chromium: Inappropriate implementation in Web Share API	High	N/A	RCE
CVE-2022-1130 *	Chromium: Insufficient validation of untrusted input in WebOTP	High	N/A	RCE
CVE-2022-1134 *	Chromium: Type Confusion in V8	High	N/A	RCE
CVE-2022-1232 *	Chromium: Type Confusion in V8	High	N/A	RCE
CVE-2022-1131 *	Chromium: Use after free in Cast UI	High	N/A	RCE
CVE-2022-1125 *	Chromium: Use after free in Portals	High	N/A	RCE
CVE-2022-1127 *	Chromium: Use after free in QR Code Generator	High	N/A	RCE
CVE-2022-1133 *	Chromium: Use after free in WebRTC	High	N/A	RCE
CVE-2022-1143 *	Chromium: Heap buffer overflow in WebUI	Medium	N/A	RCE
CVE-2022-1139 *	Chromium: Inappropriate implementation in Background Fetch API	Medium	N/A	N/A
CVE-2022-1137 *	Chromium: Inappropriate implementation in Extensions	Medium	N/A	N/A
CVE-2022-1138 *	Chromium: Inappropriate implementation in Web Cursor	Medium	N/A	N/A
CVE-2022-1145 *	Chromium: Use after free in Extensions	Medium	N/A	RCE
CVE-2022-1135 *	Chromium: Use after free in Shopping Cart	Medium	N/A	RCE
CVE-2022-1136 *	Chromium: Use after free in Tab Strip	Medium	N/A	RCE
CVE-2022-1146 *	Chromium: Inappropriate implementation in Resource Timing	Low	N/A	EoP

Impact

- Privilege Escalation
- Remote Code Execution
- Denial of Service
- Information Disclosure

Indicator Of Compromise

CVE

- CVE-2022-24521
- CVE-2022-26904
- CVE-2022-23259
- CVE-2022-26809
- CVE-2022-22008

- CVE-2022-23257
- CVE-2022-24537
- CVE-2022-26919
- CVE-2022-24491
- CVE-2022-24497
- CVE-2022-24541
- CVE-2022-24500
- CVE-2022-26832
- CVE-2022-26907
- CVE-2022-26896
- CVE-2022-26897
- CVE-2022-26898
- CVE-2022-24489
- CVE-2022-24479
- CVE-2022-26830
- CVE-2022-24767
- CVE-2022-24765
- CVE-2022-24532
- CVE-2022-24496
- CVE-2022-24548
- CVE-2022-24475
- CVE-2022-26891
- CVE-2022-26894
- CVE-2022-26895
- CVE-2022-26900
- CVE-2022-26908
- CVE-2022-24473
- CVE-2022-26901
- CVE-2022-26924
- CVE-2022-24493
- CVE-2022-23292
- CVE-2022-24472
- CVE-2022-26788
- CVE-2022-24533
- CVE-2022-24492
- CVE-2022-24528
- CVE-2022-26910
- CVE-2022-26911
- CVE-2022-26921
- CVE-2022-24513
- CVE-2022-24485
- CVE-2022-21983
- CVE-2022-24534
- CVE-2022-26914
- CVE-2022-24482
- CVE-2022-24540
- CVE-2022-24494
- CVE-2022-24549
- CVE-2022-26828
- CVE-2022-24484
- CVE-2022-24538
- CVE-2022-26784
- CVE-2022-24481

- CVE-2022-24488
- CVE-2022-24547
- CVE-2022-24495
- CVE-2022-26816
- CVE-2022-24536
- CVE-2022-26811
- CVE-2022-26812
- CVE-2022-26813
- CVE-2022-26814
- CVE-2022-26815
- CVE-2022-26817
- CVE-2022-26818
- CVE-2022-26819
- CVE-2022-26820
- CVE-2022-26821
- CVE-2022-26822
- CVE-2022-26823
- CVE-2022-26824
- CVE-2022-26825
- CVE-2022-26826
- CVE-2022-26829
- CVE-2022-24546
- CVE-2022-24527
- CVE-2022-26916
- CVE-2022-26917
- CVE-2022-26918
- CVE-2022-26808
- CVE-2022-26810
- CVE-2022-26827
- CVE-2022-26920
- CVE-2022-26903
- CVE-2022-23268
- CVE-2022-22009
- CVE-2022-24490
- CVE-2022-24539
- CVE-2022-26783
- CVE-2022-26785
- CVE-2022-24499
- CVE-2022-24530
- CVE-2022-24498
- CVE-2022-24486
- CVE-2022-24544
- CVE-2022-24545
- CVE-2022-24483
- CVE-2022-26831
- CVE-2022-24487
- CVE-2022-26786
- CVE-2022-26787
- CVE-2022-26789
- CVE-2022-26790
- CVE-2022-26791
- CVE-2022-26792
- CVE-2022-26793

- CVE-2022-26794
- CVE-2022-26795
- CVE-2022-26796
- CVE-2022-26797
- CVE-2022-26798
- CVE-2022-26801
- CVE-2022-26802
- CVE-2022-26803
- CVE-2022-26915
- CVE-2022-24550
- CVE-2022-24543
- CVE-2022-24474
- CVE-2022-24542
- CVE-2022-26807
- CVE-2022-26909
- CVE-2022-26912
- CVE-2022-24523
- CVE-2022-1129
- CVE-2022-1128
- CVE-2022-1130
- CVE-2022-1134
- CVE-2022-1232
- CVE-2022-1131
- CVE-2022-1125
- CVE-2022-1127
- CVE-2022-1133
- CVE-2022-1143
- CVE-2022-1139
- CVE-2022-1137
- CVE-2022-1138
- CVE-2022-1145
- CVE-2022-1135
- CVE-2022-1136
- CVE-2022-1146
-

Remediation

Refer to Microsoft Security Advisory for patch, upgrade, or suggested workaround information.

Microsoft Paches Update