| Tag | CVE ID | CVE Title | Severity |
|---|---|---|---|
| .NET Core | CVE-2023-38178 | .NET Core and Visual Studio Denial of Service Vulnerability | Important |
| .NET Core | CVE-2023-35390 | .NET and Visual Studio Remote Code Execution Vulnerability | Important |
| .NET Framework | CVE-2023-36873 | .NET Framework Spoofing Vulnerability | Important |
| ASP .NET | CVE-2023-38180 | .NET and Visual Studio Denial of Service Vulnerability | Important |
| ASP.NET | CVE-2023-36899 | ASP.NET Elevation of Privilege Vulnerability | Important |
| ASP.NET and Visual Studio | CVE-2023-35391 | ASP.NET Core SignalR and Visual Studio Information Disclosure Vulnerability | Important |
| Azure Arc | CVE-2023-38176 | Azure Arc-Enabled Servers Elevation of Privilege Vulnerability | Important |
| Azure DevOps | CVE-2023-36869 | Azure DevOps Server Spoofing Vulnerability | Important |
| Azure HDInsights | CVE-2023-38188 | Azure Apache Hadoop Spoofing Vulnerability | Important |
| Azure HDInsights | CVE-2023-35393 | Azure Apache Hive Spoofing Vulnerability | Important |
| Azure HDInsights | CVE-2023-35394 | Azure HDInsight Jupyter Notebook Spoofing Vulnerability | Important |
| Azure HDInsights | CVE-2023-36881 | Azure Apache Ambari Spoofing Vulnerability | Important |
| Azure HDInsights | CVE-2023-36877 | Azure Apache Oozie Spoofing Vulnerability | Important |
| Dynamics Business Central Control | CVE-2023-38167 | Microsoft Dynamics Business Central Elevation Of Privilege Vulnerability | Important |
| Mariner | CVE-2023-35945 | Unknown | Unknown |
| Memory Integrity System Readiness Scan Tool | ADV230004 | Memory Integrity System Readiness Scan Tool Defense in Depth Update | Moderate |
| Microsoft Dynamics | CVE-2023-35389 | Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability | Important |
| Microsoft Edge (Chromium-based) | CVE-2023-38157 | Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability | Moderate |
| Microsoft Edge (Chromium-based) | CVE-2023-4068 | Chromium: CVE-2023-4068 Type Confusion in V8 | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4072 | Chromium: CVE-2023-4072 Out of bounds read and write in WebGL | Unknown |

| | | | |
|---|---|---|---|
| Microsoft Edge (Chromium-based) | CVE-2023-4071 | Chromium: CVE-2023-4071 Heap buffer overflow in Visuals | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4073 | Chromium: CVE-2023-4073 Out of bounds memory access in ANGLE | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4075 | Chromium: CVE-2023-4075 Use after free in Cast | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4074 | Chromium: CVE-2023-4074 Use after free in Blink Task Scheduling | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4076 | Chromium: CVE-2023-4076 Use after free in WebRTC | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4077 | Chromium: CVE-2023-4077 Insufficient data validation in Extensions | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4078 | Chromium: CVE-2023-4078 Inappropriate implementation in Extensions | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4070 | Chromium: CVE-2023-4070 Type Confusion in V8 | Unknown |
| Microsoft Edge (Chromium-based) | CVE-2023-4069 | Chromium: CVE-2023-4069 Type Confusion in V8 | Unknown |
| Microsoft Exchange Server | CVE-2023-38185 | Microsoft Exchange Server Remote Code Execution Vulnerability | Important |
| Microsoft Exchange Server | CVE-2023-35388 | Microsoft Exchange Server Remote Code Execution Vulnerability | Important |
| Microsoft Exchange Server | CVE-2023-35368 | Microsoft Exchange Remote Code Execution Vulnerability | Important |
| Microsoft Exchange Server | CVE-2023-38181 | Microsoft Exchange Server Spoofing Vulnerability | Important |
| Microsoft Exchange Server | CVE-2023-38182 | Microsoft Exchange Server Remote Code Execution Vulnerability | Important |
| Microsoft Exchange Server | CVE-2023-21709 | Microsoft Exchange Server Elevation of Privilege Vulnerability | Important |
| Microsoft Office | ADV230003 | Microsoft Office Defense in Depth Update | Moderate |
| Microsoft Office | CVE-2023-36897 | Visual Studio Tools for Office Runtime Spoofing Vulnerability | Important |
| Microsoft Office Excel | CVE-2023-36896 | Microsoft Excel Remote Code Execution Vulnerability | Important |
| Microsoft Office Excel | CVE-2023-35371 | Microsoft Office Remote Code Execution Vulnerability | Important |
| Microsoft Office Outlook | CVE-2023-36893 | Microsoft Outlook Spoofing Vulnerability | Important |

| | | | |
|---|---|---|---|
| Microsoft Office Outlook | CVE-2023-36895 | Microsoft Outlook Remote Code Execution Vulnerability | **Critical** |
| Microsoft Office SharePoint | CVE-2023-36891 | Microsoft SharePoint Server Spoofing Vulnerability | Important |
| Microsoft Office SharePoint | CVE-2023-36894 | Microsoft SharePoint Server Information Disclosure Vulnerability | Important |
| Microsoft Office SharePoint | CVE-2023-36890 | Microsoft SharePoint Server Information Disclosure Vulnerability | Important |
| Microsoft Office SharePoint | CVE-2023-36892 | Microsoft SharePoint Server Spoofing Vulnerability | Important |
| Microsoft Office Visio | CVE-2023-35372 | Microsoft Office Visio Remote Code Execution Vulnerability | Important |
| Microsoft Office Visio | CVE-2023-36865 | Microsoft Office Visio Remote Code Execution Vulnerability | Important |
| Microsoft Office Visio | CVE-2023-36866 | Microsoft Office Visio Remote Code Execution Vulnerability | Important |
| Microsoft Teams | CVE-2023-29328 | Microsoft Teams Remote Code Execution Vulnerability | **Critical** |
| Microsoft Teams | CVE-2023-29330 | Microsoft Teams Remote Code Execution Vulnerability | **Critical** |
| Microsoft WDAC OLE DB provider for SQL | CVE-2023-36882 | Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability | Important |
| Microsoft Windows | CVE-2023-20569 | AMD: CVE-2023-20569 Return Address Predictor | Important |
| Microsoft Windows Codecs Library | CVE-2023-38170 | HEVC Video Extensions Remote Code Execution Vulnerability | Important |
| Reliability Analysis Metrics Calculation Engine | CVE-2023-36876 | Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability | Important |
| Role: Windows Hyper-V | CVE-2023-36908 | Windows Hyper-V Information Disclosure Vulnerability | Important |
| SQL Server | CVE-2023-38169 | Microsoft OLE DB Remote Code Execution Vulnerability | Important |
| Tablet Windows User Interface | CVE-2023-36898 | Tablet Windows User Interface Application Core Remote Code Execution Vulnerability | Important |
| Windows Bluetooth A2DP driver | CVE-2023-35387 | Windows Bluetooth A2DP driver Elevation of Privilege Vulnerability | Important |

| | | | |
|---|---|---|---|
| Windows Cloud Files Mini Filter Driver | CVE-2023-36904 | Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability | Important |
| Windows Common Log File System Driver | CVE-2023-36900 | Windows Common Log File System Driver Elevation of Privilege Vulnerability | Important |
| Windows Cryptographic Services | CVE-2023-36907 | Windows Cryptographic Services Information Disclosure Vulnerability | Important |
| Windows Cryptographic Services | CVE-2023-36906 | Windows Cryptographic Services Information Disclosure Vulnerability | Important |
| Windows Defender | CVE-2023-38175 | Microsoft Windows Defender Elevation of Privilege Vulnerability | Important |
| Windows Fax and Scan Service | CVE-2023-35381 | Windows Fax Service Remote Code Execution Vulnerability | Important |
| Windows Group Policy | CVE-2023-36889 | Windows Group Policy Security Feature Bypass Vulnerability | Important |
| Windows HTML Platform | CVE-2023-35384 | Windows HTML Platforms Security Feature Bypass Vulnerability | Important |
| Windows Kernel | CVE-2023-35359 | Windows Kernel Elevation of Privilege Vulnerability | Important |
| Windows Kernel | CVE-2023-38154 | Windows Kernel Elevation of Privilege Vulnerability | Important |
| Windows Kernel | CVE-2023-35382 | Windows Kernel Elevation of Privilege Vulnerability | Important |
| Windows Kernel | CVE-2023-35386 | Windows Kernel Elevation of Privilege Vulnerability | Important |
| Windows Kernel | CVE-2023-35380 | Windows Kernel Elevation of Privilege Vulnerability | Important |
| Windows LDAP - Lightweight Directory Access Protocol | CVE-2023-38184 | Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability | Important |
| Windows Message Queuing | CVE-2023-36909 | Microsoft Message Queuing Denial of Service Vulnerability | Important |
| Windows Message Queuing | CVE-2023-35376 | Microsoft Message Queuing Denial of Service Vulnerability | Important |
| Windows Message Queuing | CVE-2023-38172 | Microsoft Message Queuing Denial of Service Vulnerability | Important |
| Windows Message Queuing | CVE-2023-35385 | Microsoft Message Queuing Remote Code Execution Vulnerability | **Critical** |
| Windows Message Queuing | CVE-2023-35383 | Microsoft Message Queuing Information Disclosure Vulnerability | Important |

| | | | |
|---|---|---|---|
| Windows Message Queuing | CVE-2023-36913 | Microsoft Message Queuing Information Disclosure Vulnerability | Important |
| Windows Message Queuing | CVE-2023-35377 | Microsoft Message Queuing Denial of Service Vulnerability | Important |
| Windows Message Queuing | CVE-2023-38254 | Microsoft Message Queuing Denial of Service Vulnerability | Important |
| Windows Message Queuing | CVE-2023-36911 | Microsoft Message Queuing Remote Code Execution Vulnerability | **Critical** |
| Windows Message Queuing | CVE-2023-36910 | Microsoft Message Queuing Remote Code Execution Vulnerability | **Critical** |
| Windows Message Queuing | CVE-2023-36912 | Microsoft Message Queuing Denial of Service Vulnerability | Important |
| Windows Mobile Device Management | CVE-2023-38186 | Windows Mobile Device Management Elevation of Privilege Vulnerability | Important |
| Windows Projected File System | CVE-2023-35378 | Windows Projected File System Elevation of Privilege Vulnerability | Important |
| Windows Reliability Analysis Metrics Calculation Engine | CVE-2023-35379 | Reliability Analysis Metrics Calculation Engine (RACEng) Elevation of Privilege Vulnerability | Important |
| Windows Smart Card | CVE-2023-36914 | Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability | Important |
| Windows System Assessment Tool | CVE-2023-36903 | Windows System Assessment Tool Elevation of Privilege Vulnerability | Important |
| Windows Wireless Wide Area Network Service | CVE-2023-36905 | Windows Wireless Wide Area Network Service (WwanSvc) Information Disclosure Vulnerability | Important |